

[NOT YET SCHEDULED FOR ORAL ARGUMENT]

No. 05-5388

---

IN THE UNITED STATES COURT OF APPEALS  
FOR THE DISTRICT OF COLUMBIA CIRCUIT

---

ELOUISE PEPION COBELL, et al.,  
Plaintiffs-Appellees,  
v.

GALE A. NORTON, SECRETARY OF THE INTERIOR, et al.,  
Defendants-Appellants.

---

ON APPEAL FROM THE UNITED STATES  
DISTRICT COURT FOR THE DISTRICT OF COLUMBIA

---

BRIEF FOR THE APPELLANTS

---

PETER D. KEISLER  
Assistant Attorney General

KENNETH L. WAINSTEIN  
United States Attorney

GREGORY G. KATSAS  
Deputy Assistant Attorney General

ROBERT E. KOPP  
MARK B. STERN  
THOMAS M. BONDY  
ALISA B. KLEIN  
MARK R. FREEMAN  
I. GLENN COHEN  
ISAAC J. LIDSKY  
(202) 514-5089  
Attorneys, Appellate Staff  
Civil Division, Room 7531  
Department of Justice  
950 Pennsylvania Ave., N.W.  
Washington, D.C. 20530-0001

---

**CERTIFICATE AS TO PARTIES, RULINGS, AND RELATED CASES**

Pursuant to Circuit Rule 28(a)(1), undersigned counsel certifies as follows:

**A. Parties and Amici:**

The named plaintiffs-appellees in this class action are Elouise Pepion Cobell; Earl Old Person; Penny Cleghorn; Thomas Maulson; and James Louis Larose. The district court has certified a plaintiff class consisting of present and former beneficiaries of Individual Indian Money accounts, excluding those who had filed their own actions prior to the filing of the complaint in this case.

The defendants-appellants are Gale A. Norton, as Secretary of the Interior; the Assistant Secretary of Interior-Indian Affairs; and John W. Snow, as Secretary of Treasury.


**B. Rulings Under Review:**

Appellants seek review of the opinion and order issued on October 20, 2005, by Judge Royce C. Lamberth, United States District Court for the District of Columbia, in Civ. No. 96-1285 (RCL). The opinion and order are published at 394 F. Supp. 2d 164.

**C. Related Cases:**

This Court has issued six decisions in appeals arising out of this litigation. See Cobell v. Norton, 428 F.3d 1070 (D.C. Cir. 2005); Cobell v. Norton, 392 F.3d 461 (D.C. Cir. 2004); Cobell v. Norton, 391 F.3d 251 (D.C. Cir. 2004); In re Brooks, 383 F.3d 1036 (D.C. Cir. 2004); Cobell v. Norton, 334 F.3d 1128 (D.C. Cir. 2003); and Cobell v. Norton, 240 F.3d 1081 (D.C. Cir.

2001). In addition to this appeal, two other appeals are currently pending. See In re Norton, No. 03-5288 (oral argument heard October 14, 2005); Cobell v. Norton, No. 05-5269 (not yet scheduled for oral argument).

  
THOMAS M. BONDY  
Attorney

## TABLE OF CONTENTS

### Page

CERTIFICATE AS TO PARTIES, RULINGS, AND RELATED CASES

GLOSSARY

STATEMENT OF JURISDICTION .....	1
STATEMENT OF THE ISSUE .....	1
STATEMENT OF THE CASE .....	2
STATEMENT OF FACTS .....	4
I. General Background .....	4
A. This Court's Initial 2001 Decision .....	5
B. This Court's 2003 Contempt Decision .....	6
C. This Court's 2004 Structural Injunction Decision .....	7
D. Reissuance of the Structural Injunction .....	8
E. Mandamus Petitions Seeking Disqualification Of Special Master Balaran .....	9
F. Pending Appeal From The Order Of July 12, 2005. ....	10
II. Computer Disconnection Orders Prior to 2005 . ....	11
A. The 2001 Temporary Restraining Order .....	11
B. The 2003 and 2004 Disconnection Orders .....	12
III. The October 20, 2005 Disconnection Order .....	13
A. Statutory Provisions Governing Information Security. ....	13
B. District Court Proceedings .....	14

1. Testing by the Inspector General .....	14
2. The Order and Injunction .....	15
SUMMARY OF ARGUMENT .....	19
STANDARD OF REVIEW .....	23
ARGUMENT .....	24
I. The District Court Improperly Set Aside The Information Safety Plan Developed Under The Comprehensive FISMA Scheme And Wrongly Assumed Authority For Directing Agency Security .....	24
A. The FISMA Establishes A Highly Discretionary Comprehensive Scheme Of Cost-Effective Risk Assessment .....	24
B. Governmentwide Experience Under The FISMA Underscores The Difficulty And Complexity Of The Security Problems Faced By Agencies And OMB. ....	29
C. The Record Provides No Basis For Continuing Judicial Intervention In Computer Security ...	32
1. A Court Should Properly Defer To Decisions Taken As Part Of The FISMA Scheme .....	32
2. No Basis Exists For Setting Aside Executive Branch Security Decisions And Substituting Judicial Controls .....	34
a. The Record Demonstrates Unstinting Commitment To The FISMA Process And Substantial Progress In IT Security .....	34
b. The Problems Cited By The District Court Provide No Basis For Judicial Intervention .....	36

3.	No Evidence Exists Of Past Or Imminent Threats To Accountholder Security That Would Warrant Judicial Intervention .....	39
4.	The District Court's Belief That IITD Should Be "Segregated" Reflects a Fundamental Misunderstanding Of Computer Systems And Limitations Of Judicial Expertise .....	41
D.	In Assuming Control Of Interior Computer Systems, The District Court Replicated The Errors Underlying Its Previous Structural Injunctions .....	44
II.	The Injunction Cannot Be Reconciled With Basic Principles of Equity .....	49
A.	The Injunction Is In No Meaningful Way "Preliminary." .....	49
B.	An Injunction Must Take Into Account The Public Interest And Be Tailored To Limit Its Adverse Impact On The Defendant .....	50
C.	Plaintiffs Have Failed To Demonstrate That An Injunction Is Needed To Avoid Likely Irreparable Harm .....	58
	CONCLUSION .....	61
	CERTIFICATE OF COMPLIANCE WITH RULE 32(a)(7)(c) OF THE FEDERAL RULES OF APPELLATE PROCEDURE	
	CERTIFICATE OF SERVICE	
	STATUTORY ADDENDUM	

## TABLE OF AUTHORITIES

Cases:	<u>Page</u>
<u>In re Barr Laboratories, Inc.</u> , 930 F.2d 72 (D.C. Cir. 1991) .....	33
<u>In re Brooks</u> , 383 F.3d 1036 (D.C. Cir. 2004) .....	9
<u>Central &amp; Southern Motor Freight Tariff Ass'n v. United States</u> , 757 F.2d 301 (D.C. Cir. 1985) .....	33
<u>Cobell v. Babbitt</u> , 91 F. Supp. 2d 1 (D.D.C. 1999) .....	5
<u>Cobell v. Norton</u> , 226 F. Supp. 2d 1 (D.D.C. 2002) .....	6
<u>Cobell v. Norton</u> , 226 F. Supp. 2d 163 (D.D.C. 2002) .....	6
<u>Cobell v. Norton</u> , 274 F. Supp. 2d 111 (D.D.C. 2003) .....	3, 12
<u>Cobell v. Norton</u> , 283 F. Supp. 2d 66 (D.D.C. 2003) .....	7
<u>Cobell v. Norton</u> , 310 F. Supp. 2d 98 (D.D.C. 2004) .....	3, 12
<u>Cobell v. Norton</u> , 357 F. Supp. 2d 298 (D.D.C. 2005) .....	8
<u>Cobell v. Norton</u> , 229 F.R.D. 5 (D.D.C. 2005) .....	10
<u>Cobell v. Norton</u> , 394 F. Supp. 2d 164 (D.D.C. 2005) .....	<u>passim</u>
<u>Cobell v. Norton</u> , 240 F.3d 1081 (D.C. Cir. 2001) .....	5, 59
<u>Cobell v. Norton</u> , 334 F.3d 1128 (D.C. Cir. 2003) .....	6
<u>Cobell v. Norton</u> , 391 F.3d 251 (D.C. Cir. 2004) ....	3, 12, 59
* <u>Cobell v. Norton</u> , 392 F.3d 461 (D.C. Cir. 2004) .....	8, 22, 33, 46, 47
* <u>Cobell v. Norton</u> , 428 F.3d 1070 (D.C. Cir. 2005) .....	7, 8, 20, 23, 33 44, 47

---

\* Authorities chiefly relied upon are marked with an asterisk.

<u>Heckler v. Chaney</u> , 470 U.S. 821 (1985) .....	33
<u>Koon v. United States</u> , 518 U.S. 81 (1996) .....	24
* <u>Norton v. Southern Utah Wilderness Alliance</u> , 542 U.S. 55 (2004) .....	8, 9, 33, 47
<u>Steel Manufacturers Ass'n v. EPA</u> , 27 F.3d 642 (D.C. Cir. 1994) .....	33
<u>Udall v. D.C. Transit System, Inc.</u> , 404 F.2d 1358 (D.C. Cir. 1968) .....	50
<u>University of Texas v. Camenisch</u> , 451 U.S. 390 (1981) .....	50
<u>Washington Metropolitan Area Transit Comm'n v. Holiday Tours, Inc.</u> , 559 F.2d 841 (D.C. Cir. 1977) .....	50
<u>Weinberger v. Romero-Barcelo</u> , 456 U.S. 305 (1982) .....	50
<u>Wisconsin Gas Co. v. FERC</u> , 758 F.2d 669 (D.C. Cir. 1985) ..	58

#### **Statutes:**

American Indian Trust Fund Management Reform Act, Pub. L. No. 103-412, 108 Stat. 4239 .....	4
Pub. L. No. 108-108 .....	7
117 Stat. 1263 .....	8
5 U.S.C. App.3 .....	25
5 U.S.C. § 706(1) .....	5
18 U.S.C. § 1030 .....	40
28 U.S.C. § 1292(a) .....	1
28 U.S.C. § 1331 .....	1
28 U.S.C. § 1361 .....	1
44 U.S.C. § 3541(1) .....	13
* 44 U.S.C. § 3543 .....	27
44 U.S.C. § 3543(a) .....	14, 27
44 U.S.C. § 3543(a)(5) .....	14, 25



* 44 U.S.C. § 3544 .....	27
44 U.S.C. § 3544 (a) (1) (A) .....	13, 24, 28
44 U.S.C. § 3544 (a) (1) (C) .....	13, 24
44 U.S.C. § 3544 (a) (2) .....	24
44 U.S.C. § 3544 (a) (2) (B) .....	25
44 U.S.C. § 3544 (b) (2) (A) .....	13, 25
44 U.S.C. § 3544 (b) (2) (B) .....	13, 25
44 U.S.C. § 3544 (b) (8) .....	29
44 U.S.C. § 3544 (c) .....	25
44 U.S.C. § 3544 (c) (1) .....	14
* 44 U.S.C. § 3545 .....	14, 25
44 U.S.C. § 3545 (a) (1) .....	14, 25
44 U.S.C. § 3545 (b) (1) .....	13, 25

#### **Miscellaneous:**

2004 Subcommittee Scorecard, <a href="http://reform.house.gov/UploadedFiles/2004%20Computer%20Security%20Report%20card%20%20years.pdf">http://reform.house.gov/UploadedFiles/2004%20Computer%20Security%20Report%20card%20%20years.pdf</a> .....	29
<u>40 Million Cards May Be Affected By Breach</u> , Washington Post, 6/19/05, at A21 .....	31
Associated Press, <u>Computer Breach at U. of Connecticut</u> , N.Y. Times, 6/25/05, at C13 .....	31
<u>Hacker Accesses USC Files</u> , L.A. Times, 7/9/05, at B3 .....	31
Identity Theft Resource Center, <a href="http://www.idtheftcenter.org/breaches.pdf">http://www.idtheftcenter.org/breaches.pdf</a> .....	31
Information Technology, DOD FY 2004 Implementation of FISMA, <a href="http://www.dodig.osd.mil/Audit/reports/FY05/05-025.pdf">http://www.dodig.osd.mil/Audit/reports/FY05/05-025.pdf</a> .	30-31
NIST Special Publication 800-30 .....	27
NIST Special Publication 800-37 .....	26
OMB Circular A-130, App. III .....	25, 26, 28, 56
Privacy Rights Clearinghouse, A Chronology of Data Breaches Reported Since the ChoicePoint Incident, <a href="http://www.privacyrights.org/ar/ChronDataBreaches.htm">http://www.privacyrights.org/ar/ChronDataBreaches.htm</a> ....	31
Restatement (Second) of Trusts (1959) .....	46

## GLOSSARY

1994 Act	American Indian Trust Fund Management Reform Act
APA	Administrative Procedure Act
BIA	Bureau of Indian Affairs
CIO	Chief Information Officer
FISMA	Federal Information Security Management Act
GAO	Government Accountability Office
IG	Inspector General
IIM Accounts	Individual Indian Money Accounts
IITD	Individual Indian Trust Data
IT	Information Technology
MMS	Minerals Management Service
NBC	National Business Center
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
OST	Office of Special Trustee

[NOT YET SCHEDULED FOR ORAL ARGUMENT]

IN THE UNITED STATES COURT OF APPEALS  
FOR THE DISTRICT OF COLUMBIA CIRCUIT

---

No. 05-5388

---

ELOUISE PEPION COBELL, et al.,  
Plaintiffs-Appellees,

v.

GALE A. NORTON, SECRETARY OF THE INTERIOR, et al.,  
Defendants-Appellants.

---

ON APPEAL FROM THE UNITED STATES  
DISTRICT COURT FOR THE DISTRICT OF COLUMBIA

---

BRIEF FOR THE APPELLANTS

---

**STATEMENT OF JURISDICTION**

Plaintiffs invoked the district court's jurisdiction under 28 U.S.C. §§ 1331 and 1361, inter alia. The order on appeal was issued on October 20, 2005, and styled as a preliminary injunction. 394 F. Supp. 2d 164. The government filed a timely notice of appeal on October 21, 2005. This Court has jurisdiction pursuant to 28 U.S.C. § 1292(a).

**STATEMENT OF THE ISSUE**

Whether this Court should vacate an injunction that requires components of the Department of the Interior to disconnect their computers from the internet and from internal computer networks, and that precludes some previously disconnected components from reestablishing internet access.

## STATEMENT OF THE CASE

This is an appeal from an injunction that requires the Department of the Interior to immediately sever internet connections for major computer systems now on-line and precludes reconnection of other systems already disconnected. The injunction further requires that all these systems dismantle their internal communications capacities, so that computers within a particular Interior component cannot communicate with each other or with other Interior components.

The order issued on October 20, 2005, nine years after this class action was filed in 1996, seeking relief including an accounting of funds in Individual Indian Money ("IIM") accounts. As described below, this Court has, to date, issued six published opinions in this case. Oral argument in a seventh appeal was heard in October 2005. Briefing in an eighth appeal will be completed on January 20, 2006.

The district court issued its first order with respect to computer disconnection in December 2001. Although no evidence suggested that any class member had been injured by computer tampering, the district court issued a temporary restraining order requiring Interior to immediately disconnect from the internet all computers that might provide access to Individual Indian Trust Data ("IITD"). Because such data is contained in many computer systems and because computer systems are interconnected, the TRO required broad, agencywide disconnections.

To regain internet access, Interior agreed to a consent order which set out a procedure for restoring internet connections upon agreement by the court's Special Master. Order of 12/17/01. With the Master's approval, Interior reconnected a number of major systems to the internet. However, by the time the regime established by the consent order concluded in 2003, several significant Interior components remained off-line.

In July 2003, the district court entered a preliminary injunction by which the court, rather than the Special Master, assumed full authority over internet access. Cobell v. Norton, 274 F. Supp. 2d 111 (D.D.C. 2003). In March 2004, the district court issued a superseding preliminary injunction requiring Interior immediately to disconnect its computer systems from the internet, with limited exceptions. Cobell v. Norton, 310 F. Supp. 2d 98 (D.D.C. 2004).

This Court stayed and later vacated the injunction. Cobell v. Norton, 391 F.3d 251 (D.C. Cir. 2004). Noting that "there was no evidence that anyone other than the Special Master's contractor had 'hacked' into any Interior computer system housing or accessing IITD," id. at 259, this Court remanded for further proceedings, id. at 262.

In 2005, plaintiffs again moved for an injunction, following which the district court conducted a 59-day evidentiary hearing on the security of Interior's information systems. On October 20, 2005, the district court issued a "preliminary injunction" requiring Interior "forthwith" to disconnect all computer systems

that provide access to Individual Indian Trust Data, defined broadly so that, as the court noted, "IITD is suffused in varying forms and amounts throughout Interior's network environment." Cobell v. Norton, 394 F. Supp. 2d 164, 271, 277-78 (D.D.C. 2005). This Court granted an administrative stay on October 21, 2005, and a stay pending appeal on December 9, 2005.

### **STATEMENT OF FACTS**

Because the computer disconnection order cannot be fully understood without regard to the litigation as a whole, we first briefly describe, in Section I, the prior decisions relating to accounting duties and the conduct of the case generally. In Section II, we describe prior computer disconnection orders. In Section III, we discuss the framework for government computer security oversight enacted in 2002 as the Federal Information Security Management Act ("FISMA") and the order now on appeal.

#### **I. General Background.**

The Department of the Interior administers roughly 260,000 Individual Indian Money trust accounts with balances totaling approximately \$400 million. In 1994, Congress enacted the American Indian Trust Fund Management Reform Act, Pub. L. No. 103-412, 108 Stat. 4239, which requires the Secretary of the Interior to "account for the daily and annual balance of all funds held in trust by the United States for the benefit of an Indian tribe or an individual Indian which are deposited or invested pursuant to" a 1938 statute addressing investment of trust monies. In 1996, a class of present and former IIM

accountholders filed this lawsuit, claiming among other things that the government had failed to provide a timely, adequate accounting.

**A. This Court's Initial 2001 Decision.**

In 1999, the district court issued a declaratory judgment holding that Interior has an enforceable duty to account for the balances in the IIM accounts. Cobell v. Babbitt, 91 F. Supp. 2d 1, 28-31, 56 (D.D.C. 1999). This Court's 2001 decision largely affirmed the declaratory judgment, concluding that the agency had unreasonably delayed performance of accounting activities within the meaning of 5 U.S.C. § 706(1). Cobell v. Norton, 240 F.3d 1081, 1108 (D.C. Cir. 2001).

Although this Court noted that adequate computer systems would be needed to accomplish the required accounting, 240 F.3d at 1106, neither the district court's order nor this Court's decision addressed potential problems that might be generated by computer hackers. To the extent that computer systems were at issue, the concern posed was the need for improved systems to compile and process trust data. See id. at 1092 (noting problems and new computer systems outlined in Interior's 1998 plan of operations). Even in this regard, this Court emphasized the discretion to be afforded the agency in implementing computer systems and other tasks, noting that the "actual legal breach is the failure to provide an accounting, not its failure to take the discrete individual steps that would facilitate an accounting,"

id. at 1106, and admonishing the district court "to be mindful of the limits of its jurisdiction," id. at 1110.

**B. This Court's 2003 Contempt Decision.**

The remand to the agency envisioned by this Court's decision was short-lived. By the end of 2001, following receipt of reports from Special Master-Monitor Joseph Kieffer, the district court had initiated contempt proceedings charging that Interior had failed to initiate an historical accounting and had included inaccurate statements in its quarterly reports to the court.

The district court ultimately held the Secretary and an Assistant Secretary of the Interior in contempt, declaring that "Secretary Norton and Assistant Secretary McCaleb can now rightfully take their place ... in the pantheon of unfit trustee-delegates." Cobell v. Norton, 226 F. Supp. 2d 1, 161 (D.D.C. 2002). The court announced that, henceforth, it would direct the conduct of the accounting as well as virtually all other trust activities. The court thus ordered the parties to submit accounting plans, as well as plans for achieving compliance with the government's fiduciary obligations to Indians, to be evaluated by the court with a view to issuance of structural relief. Id. at 148-49. In an accompanying ruling, the district court denied the government's motion seeking Mr. Kieffer's removal. Cobell v. Norton, 226 F. Supp. 2d 163 (D.D.C. 2002).

In Cobell v. Norton, 334 F.3d 1128 (D.C. Cir. 2003), this Court vacated the contempt citations because the record demonstrated that "in her first six months in office Secretary



Norton took significant steps toward completing an accounting," id. at 1148, and because the district court's reasoning with respect to the other charges was "mystifying," id. at 1149, and "inconceivable," id. at 1150.

The Court also vacated the appointment of Special Master-Monitor Kieffer, whose reports had prompted the contempt proceedings, id. at 1135, explaining that the district court had improperly "charged [Mr. Kieffer] with an investigative, quasi-inquisitorial, quasi-prosecutorial role that is unknown to our adversarial legal system." Id. at 1142.

**C. This Court's 2004 Structural Injunction Decision.**

The contempt trial had formed the predicate for the district court's assumption of authority and its justification for issuing structural relief. However, this Court's decision vacating the contempt ruling did not cause the district court to reconsider its action. See Cobell v. Norton, 428 F.3d 1070, 1076-77 (D.C. Cir. 2005) (discussing the district court's failure to reconsider the basis for structural relief).

The structural injunction that issued in September 2003, Cobell v. Norton, 283 F. Supp. 2d 66 (D.D.C. 2003), set aside Interior's plan for an historical accounting and established detailed new requirements that caused "the cost of complying with the injunction to rise by more than an order of magnitude, from \$335 million over five years to more than \$10 billion." 428 F.3d at 1077. In response, Congress, as part of the FY 2004 Interior appropriation, Pub. L. No. 108-108, amended applicable law,

effective until December 31, 2004, to provide that no provision of law required the performance of an historical accounting. See 117 Stat. 1263. This Court vacated the accounting provisions of the structural injunction on the basis of this legislation. Cobell v. Norton, 392 F.3d 461 (D.C. Cir. 2004).

This Court also vacated the provisions of the structural injunction establishing judicial oversight over trust management generally (with the exception of a single reporting requirement). This Court rejected the district court's premise that judicial intervention of this type was permissible because IIM accountholders are trust beneficiaries. This Court made clear that defendants' fiduciary status did not vitiate the normal structure of judicial review of agency action, id. at 471-78, stressing that the APA "'empowers a court only to compel an agency ... to take action upon a matter, without directing how it shall act.'" Id. at 475 (quoting Norton v. Southern Utah Wilderness Alliance, 542 U.S. 55, 64 (2004)).

#### **D. Reissuance of the Structural Injunction.**

In February 2005, after the appropriations provision governing historical accounting activities had expired, the district court reissued the accounting portion of the original structural injunction without modification. Cobell v. Norton, 357 F. Supp. 2d 298 (D.D.C. 2005).

This Court stayed the injunction and, in November 2005, vacated the injunction in its entirety, Cobell v. Norton, 428 F.3d 1070 (D.C. Cir. 2005), concluding that "reissuance of the

injunction was not properly grounded in either fact or law." Id. at 1076.

This Court explained that the district court "owed substantial deference to Interior's plan" for historical accounting activities, ibid., and emphasized that "[t]he choices at issue required both subject-matter expertise and judgment about the allocation of scarce resources, classic reasons for deference to administrators." Ibid. The district court, however, had improperly "invoked the common law of trusts and quite bluntly treated the character of the accounting as its domain." Ibid. It had "thus erroneously displaced Interior as the actor with primary responsibility for 'work[ing] out compliance with the broad statutory mandate.'" Ibid. (quoting Southern Utah, 542 U.S. at 66-67).

**E. Mandamus Petitions Seeking Disqualification Of Special Master Balaran.**

This Court has also considered two mandamus petitions regarding Special Master Alan Balaran. In 2004, the Court ordered Mr. Balaran recused from contempt proceedings involving 37 current and former Interior and Justice Department officials. In re Brooks, 383 F.3d 1036, 1044-46 (D.C. Cir. 2004). In 2003, for separate reasons, the government sought Mr. Balaran's recusal from all future proceedings. See No. 03-5288. In April 2004, three days before this Court was scheduled to hear oral argument on the government's mandamus petition, Mr. Balaran submitted his resignation. After further briefing, this Court heard oral argument on October 14, 2005.

**F. Pending Appeal From The Order Of July 12, 2005.**

On July 12, 2005, the district court issued an order requiring Interior to state in all written communications with class members, without regard to subject matter, that any information regarding trust assets may be unreliable. Cobell v. Norton, 229 F.R.D. 5 (D.D.C. 2005). The July 12 opinion, which had no nexus to any evidentiary proceeding, engaged in an extended diatribe against current Interior officials and employees, decrying the present Interior Department as a "dinosaur - the morally and culturally oblivious hand-me-down of a disgracefully racist and imperialist government that should have been buried a century ago, the last pathetic outpost of the indifference and anglocentrism we thought we had left behind." Id. at 7. It accused the Department of "vindictiveness" and "dishonesty," id. at 9, "Machiavellian guile," id. at 10, and "Byzantine maneuvering," id. at 11, all of which form part of a "degenerate tenure as Trustee-Delegate for the Indian trust," which has featured "scandals, deception, dirty tricks and outright villainy - the end of which is nowhere in sight," id. at 11. This Court stayed the July 12 order, and briefing in that appeal is scheduled to be completed on January 20, 2006. See No. 05-5269. Those briefs also address the government's request that the case be assigned to a different district court judge.

## **II. Computer Disconnection Orders Prior to 2005.**

### **A. The 2001 Temporary Restraining Order.**

In November 2001, at approximately the same time that the contempt proceedings were initiated, Special Master Balaran issued a report identifying flaws in Interior's computer security that the Master believed could detrimentally affect the integrity of Individual Indian Trust Data. See 394 F. Supp. 2d at 166. Although no evidence existed that any person other than the Special Master had ever hacked into Interior's systems, the court entered a temporary restraining order requiring Interior to immediately disconnect from the internet all information systems housing or providing access to IITD. Ibid. Because IITD is present on many computer systems, and because computer systems are interconnected, the order required disconnection of a host of systems, including those of the Bureau of Indian Affairs and the Office of Special Trustee, the two Interior bureaus most significantly involved with administering Indian trust matters.

To regain internet access, Interior agreed to a consent order by which it assented to a procedure for restoring internet connections. Id. at 166-67. The consent order provided that offices would be restored to the internet upon agreement by the Master that the systems were secure or that they neither housed nor provided access to IITD. Id. at 167. Ultimately, most systems taken off-line were restored. Ibid. However, by the time the Special Master regime concluded in 2003, several Interior components, including the Bureau of Indian Affairs and

the Office of Special Trustee, were still barred from internet connection.

**B. The 2003 and 2004 Disconnection Orders.**

In July 2003, the district court entered a preliminary injunction by which the court, rather than the Special Master, assumed full authority over internet access. Cobell v. Norton, 274 F. Supp. 2d 111 (D.D.C. 2003). The order made no provision for further reconnections as contemplated by the earlier consent agreement and, instead, required Interior to immediately disconnect from the internet the systems already approved by the Special Master. The court stayed the effect of its order with respect to systems that were not already off-line, to allow Interior to submit certifications showing that the systems still connected to the internet were secure from internet access by unauthorized users. Id. at 135-36.

In March 2004, without considering the government's evidence, the district court issued a preliminary injunction that superseded the 2003 injunction and required Interior immediately to disconnect all information systems from the internet, with limited exceptions. Cobell v. Norton, 310 F. Supp. 2d 98 (D.D.C. 2004).

This Court first stayed and, in December 2004, vacated the injunction. Cobell v. Norton, 391 F.3d 251 (D.C. Cir. 2004). Noting that "there was no evidence that anyone other than the Special Master's contractor had 'hacked' into any Interior

computer system housing or accessing IITD," id. at 259, this Court remanded for further proceedings, id. at 262.

### **III. The October 20, 2005 Disconnection Order.**

#### **A. Statutory Provisions Governing Information Security.**

In 2002, Congress enacted the Federal Information Security Management Act ("FISMA"), which establishes a "comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations." 44 U.S.C. § 3541(1).

1. The FISMA makes the head of each agency responsible for "providing information security protections" that are "commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction." 44 U.S.C. § 3544(a)(1)(A). These protections must be "integrated with agency strategic and operational planning processes." Id. § 3544(a)(1)(C). Each agency must "develop, document, and implement an agencywide information security program," which must include policies and procedures aimed at "cost-effectively reduc[ing] information security risks to an acceptable level" on the basis of mandated risk assessments. Id. § 3544(b)(2)(A), (B).

2. The FISMA requires an "independent evaluation of the information security program and practices of that agency," 44 U.S.C. § 3545(a)(1), which is generally performed by the agency's Inspector General ("IG"), id. § 3545(b)(1). The IG's independent evaluation includes a testing of effectiveness, and an assessment

of compliance with statutory requirements and related security policies. Id. § 3545(a)(1).

3. The FISMA vests the Office of Management and Budget ("OMB") with ultimate responsibility to "oversee agency information security policies and practices." 44 U.S.C. § 3543(a). OMB is empowered to "approv[e] or disapprov[e], agency information security programs," id. § 3543(a)(5), and the agencies and Inspector Generals are required to report to OMB at least annually, id. §§ 3544(c)(1), 3545.

**B. District Court Proceedings.**

**1. Testing by the Inspector General.**

In 2003, Interior officials contacted Interior's IG, offering to fund independent "penetration testing" of the Department's computer systems. 394 F. Supp. 2d at 202. The testing entailed the IG's retention of a team of expert security consultants to conduct a variety of simulated attacks by "hackers." Id. at 199. The IG testified that this offer allowed him "to jump start that program that I was trying desperately to find funds" to implement. Id. at 202 (quoting Devaney, 5/20/05 AM at 37).

That both Interior and the IG believed that penetration testing would provide a useful diagnostic tool reflected the extent to which progress had already been made. Prior to that time, "Interior's IT security program had simply not advanced far enough for penetration testing to be a useful evaluation tool." Id. at 200.



In April 2005, after the IG's office had started its penetration testing, Interior provided the district court with the IG's "Notice of Potential Findings and Recommendation with Respect to Information Technology Systems," which included the results of a recent penetration test. 394 F. Supp. 2d at 169. Plaintiffs immediately sought a temporary restraining order and preliminary injunction requiring disconnection of Interior's computers. Ibid.

The hearing on this motion grew into a 59-day trial. Among other witnesses, personnel from the IG's office and its contractors testified regarding their concerns with Interior's security as well as the progress that the agency had made.

## **2. The Order and Injunction.**

The district court once more issued an injunction requiring disconnection of a broad array of Interior computers and computer systems from the internet. 394 F. Supp. 2d 164. In contrast to its previous orders, however, this injunction also required that Interior sever internal connections from other Department computers, networks, or electronic devices. Id. at 276-78. Thus, some systems, such as those of the Minerals Management Service, which are currently connected to the internet, would lose both external and internal connections. Other systems, such as those of the Bureau of Indian Affairs and the Office of Special Trustee, which are already denied internet access, would be precluded from reconnection, and would also have to sever

electronic communications internally and to all other Interior components.

a. The court did not find that anyone other than the IG (and, earlier, the Special Master) had ever hacked into any relevant computer system or that any IIM accountholder had ever been injured because of a problem with Interior's computer security. It did not find that computer security at Interior was significantly different than at other government agencies. Nor did it find that Interior had failed to make progress or to commit energy and resources to enhancing computer security. To the contrary, the court observed that "[t]here can be no doubt that Interior has made substantial progress in implementing a comprehensive departmental IT security program in a very short time," 394 F. Supp. 2d at 249, and recognized that "Interior's progress in a period of five years is laudable," id. at 272. As the court also noted, Interior had invested over \$100 million in IT security in a three-year period. Id. at 267-68.

The court noted continuing problems, however, and stressed in particular that Interior's information safety plan should be structured to give the highest priority to Individual Indian Trust Data. Thus, despite the "substantial progress that has been made," the court concluded that judicial intervention was warranted because "the evidence indicates that Interior has not properly emphasized IITD in its IT security efforts." Id. at 272.

b. The injunction requires that Interior "forthwith" disconnect affected computers:

1. from the Internet;
2. from all intranet connections ... or any other connection to any other Interior bureau or office;
3. from all other Information Technology Systems; and
4. from any contractors, Tribes, or other third parties.

Id. at 277-78.

The computers subject to this disconnection are described in a series of sweeping definitions. The order requires disconnection of "all Information Technology Systems that House or provide Access to Individual Indian Trust Data." Id. at 277.

An "Information Technology System" is defined to include "[a]ny computer, server, equipment, device, network, intranet, enclave, or application, or any subsystem thereof" used by Interior in any number of ways, "including without limitation computers, wireless devices (e.g. Blackberrys) and networks," as well as any "ancillary equipment, devices, or similar services or protocols." Id. at 276-77.

"Individual Indian Trust Data" is not limited to records of IIM account balances, withdrawals, and deposits. Instead, it encompasses all "[i]nformation ... that evidences, embodies, refers to, or relates to – directly or indirectly and generally or specifically – a Federal Record that reflects the existence of Individual Indian Trust Assets," provided that this information was used or produced in some way related to the administration of

the trust or in Interior's relationship with individual Indian trust beneficiaries. Id. at 277 (emphasis added).

In turn, "Federal Record" includes all federal documentary materials in any physical form whatsoever that are preserved, or are appropriate for preservation, because of their informational content. Ibid.

"Individual Indian Trust Assets" include all lands, natural resources, monies, and other assets held in trust for individual Indians by the federal government. Ibid.

The district court fully understood the breadth of the resulting injunctive provisions. As it observed, "IITD in one form or another permeates Interior's IT environment fairly completely," id. at 258; see also id. at 271 ("The evidence shows that IITD is suffused in varying forms and amounts throughout Interior's network environment.").

The injunction exempts from its scope only those systems "necessary for protection against fires or other such threats to life, property, or national security." Id. at 278.

The order purports to mitigate its impact by allowing Interior to reconnect computer systems for up to five business days per month "for the purpose of receiving and distributing trust funds, or for the purpose of conducting other necessary financial transactions." Ibid. Before it may do so, Interior must provide five days advance notice to the court and to the plaintiffs, together with a plan for interim "security controls and measures to cover such reconnection." Id. at 279.

The order will continue indefinitely unless and until Interior persuades the court to authorize connection of one or more systems. Interior may urge such reconnections in proposals that include "a uniform standard to be used to evaluate the security of all Information Technology Systems which House or provide Access to Individual Indian Trust Data[.]" Ibid.

Each proposal will then become the subject of additional adversary litigation. The plaintiffs are authorized to take discovery regarding the proposal, following which the district court "will conduct any necessary evidentiary hearing and decide whether a proposed Information Technology System may be reconnected and order further relief, as appropriate." Ibid.

c. On October 21, 2005, this Court granted the government's motion for an administrative stay. On December 9, 2005, the Court issued a stay pending appeal and granted the government's motion for expedition.

#### **SUMMARY OF ARGUMENT**

The district court has required a Cabinet department to disassemble much of its electronic communications network, severing links to the public and other federal agencies, and dismantling bureau-to-bureau and computer-to-computer connections with respect to affected components. Although the purpose of the injunction is different, its effect is the same as an act of computer sabotage designed to bring a government agency to its knees. The 59-day trial established no legal or factual basis

for any order of relief. Separately, the injunction fails both as a matter of law and if judged solely by principles of equity.

I. The Federal Information Security Management Act, enacted in 2002, establishes a comprehensive framework for addressing computer security that directs agency officials to evaluate risks, prioritize their concerns, and develop cost-effective solutions to the most pressing problems. It does not establish substantive standards of security, and does not suggest (much less require) that sweeping computer disconnections may be an appropriate means for achieving security improvements.

A court undertaking review of decisions made under the FISMA scheme should recognize that "[t]he choices at issue required both subject-matter expertise and judgment about the allocation of scarce resources, classic reasons for deference to administrators." 428 F.3d at 1076. The need for deference is underscored by a statutory structure that explicitly requires responsible officials to balance costs and risks and develop priorities on an agencywide basis. The comprehensive review mechanisms including independent Inspector General assessments and OMB oversight provide additional reasons to defer to Executive Branch choices. Indeed, a court that addresses an agency security plan reviews no single decision but a program of multiple, interrelated technical strategies that reflect a series of risk and cost assessments.

The 59-day trial provided no basis for rejecting Executive Branch security decisions in favor of judicial controls.

As the district court acknowledged, Interior has invested over \$100 million in IT security in three years, and has made real and substantial progress in implementing an IT security program. In so doing, Interior has made every effort to implement the FISMA process as Congress intended. The IG's "penetration testing" that formed the focus of the trial was undertaken at Interior's invitation and made possible by its funding.

As might reasonably have been expected, the testing revealed weaknesses as well as strengths. However, the IG's evidence and the record as a whole make clear that the problems faced by Interior are not different in severity or kind than those facing federal agencies in general. More important, the record demonstrates both commitment to information security and significant actual progress, and does not suggest that any judicial action is required to ensure that the Executive Branch mechanisms function as Congress contemplated.

The district court nevertheless frankly declared that it could reorder agency priorities because Interior has a fiduciary relationship with IIM accountholders. That error replicates the mistaken premise of previous structural injunctions, and this Court has explicitly held that the court may not substitute its judgment for that of the agency by invoking the status of accountholders as trust beneficiaries. Moreover, the court's belief that the agency should shift priorities by "segregating" its Indian trust data reflects its pervasive misunderstanding of

complex computer systems and underscores why courts defer to Executive Branch judgments in this area.

The court thus erred in believing that any basis existed for setting aside the agency's information security program or undertaking further judicial intervention. The court did not, however, merely purport to set aside Interior's program. Instead, as in its previous structural injunctions, the district court disregarded this Court's declaration that a court is empowered only to compel an agency "'take action upon a matter, without directing how it shall act,'" 392 F.3d at 475, and that it should not interject itself "into day-to-day agency management," id. at 472. The court thus mandated its own security program, which includes widespread, crippling disconnections that would remain in effect until the government persuaded the court in further adversarial proceedings that the court should, in its discretion, permit reconnections. The record provides no legal or factual basis for any relief, much less the injunction issued by the court.

II. Apart from these errors, however, it would be necessary to vacate the injunction even it were judged solely by standards of equity: the injunction would result in immediate and crushing harm to the public interest and is not required to prevent imminent, irreparable harm to plaintiffs.

The order requires both external and internal computer disconnections. Some major systems, such as those of the Minerals Management Service, must sever their internet



connections. Other components, such as the Bureau of Indian Affairs and the Office of Special trustee, are precluded from reconnecting. All affected components must sever their connections with each other and with the rest of the Department, and must also disassemble their own internal, computer-to-computer communications. The precise impact of the order is discussed below, but the general devastation of government services that would result should not require elaboration. The court's suggestion that the impact of the injunction would be mitigated by allowing reconnections for five days each month betrays a deep misunderstanding of the operation of these systems and is without a foothold in common sense.

That the court would issue such an order is even more extraordinary because plaintiffs have made no showing that the injunction is required to avoid any imminent harm, much less significant or irreparable harm. The record is barren of even a single instance in which an IIM accountholder has been harmed by the activities of an unauthorized hacker. Plaintiffs do not satisfy the threshold requirement for any equitable relief, much less the relief ordered by the court.

#### **STANDARD OF REVIEW**

Legal conclusions underlying an injunction are reviewed de novo. Cobell, 428 F.3d at 1074. Although the decision to enter an injunction is reviewed for abuse of discretion, ibid., a court necessarily abuses its discretion when it fails to apply proper

legal standards. Koon v. United States, 518 U.S. 81, 100 (1996). Any pertinent factual findings would be reviewed for clear error.

#### **ARGUMENT**

- I. The District Court Improperly Set Aside The Information Safety Plan Developed Under The Comprehensive FISMA Scheme And Wrongly Assumed Authority For Directing Agency Security.**
- A. The FISMA Establishes A Highly Discretionary Comprehensive Scheme Of Cost-Effective Risk Assessment.**

1. The Federal Information Security Management Act establishes a comprehensive scheme for promoting and monitoring computer security throughout the federal government. The statute creates procedures rather than substantive mandates. At every point, it stresses that agencies must evaluate security concerns in an integrated manner, and must weigh costs and risks.

Each agency is thus responsible for providing information security protections "commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction." 44 U.S.C.

§ 3544(a)(1)(A). These protections must be implemented through security processes that are "integrated with agency strategic and operational planning processes." Id. § 3544(a)(1)(C). The statute emphasizes that agencies should assess "the risk and magnitude of the harm that could result" from potential security problems, and implement "policies and procedures to cost-effectively reduce risks to an acceptable level[.]" Id. § 3544(a)(2). Similarly, the statute provides that the agency

information security program should include policies and procedures aimed at "cost-effectively reduc[ing] information security risks to an acceptable level" on the basis of the required risk assessments. Id. § 3544(b)(2)(A), (B).

Although the FISMA vests primary responsibility in responsible agency officials, it also requires an "independent evaluation of the information security program and practices of that agency," 44 U.S.C. § 3545(a)(1), and specifies that this annual audit should, when possible, be performed by the agency's Inspector General, id. § 3545(b)(1). Like the agency's own assessments, the IG's evaluations are provided to congressional oversight committees. Id. §§ 3544(c), 3545. These provisions reflect the IG's general statutory function as a largely independent office within an executive agency charged with investigating agency operations in order to assist Congress and the agency by recommending means of improving economy and efficiency. 5 U.S.C. App.3 § 4(a)(1)&(3).

The FISMA provides not only for an independent IG role and congressional oversight, but also for ultimate review authority in the Executive Branch by OMB. Both the agency and the IG must report to OMB at least annually, 44 U.S.C. §§ 3544(c), 3545, and OMB has final authority to "approv[e]" or "disapprov[e]" information security plans, id. § 3543(a)(5).

2. The FISMA procedures incorporate guidance issued by OMB and by the National Institute of Standards and Technology ("NIST"). See 44 U.S.C. § 3544(a)(2)(B). Like provisions of the

statute, this guidance is procedural and does not purport to establish substantive criteria. OMB's security policies are premised on the core concept of "adequate security," which OMB has defined to mean "security commensurate with the risk and magnitude of the [potential] harm." OMB Circular A-130, App. III, § A(2)(a). "This definition explicitly emphasizes the risk-based policy for cost-effective security established by the Computer Security Act[,] " id. § B; see 394 F. Supp. 2d at 171.

NIST standards establish a process by which risks should be assessed and managed, including a "certification," which is defined as "a comprehensive assessment of the management, operational, and technical security controls in an information system[.]" NIST Special Publication 800-37 at 1; see 394 F. Supp. 2d at 172. On the basis of this information, a designated agency official must make a decision whether an information system warrants "accreditation." The purpose of the NIST certification and accreditation process is to assure responsible risk assessment and accountability. Thus, an agency's accreditation decision is "the official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations, agency assets, or individuals based on the implementation of an agreed-upon set of security controls." NIST SP 800-37 at 1.

NIST guidance explains that, for purposes of information security management, an agency's risk assessment should reflect

the nature of the information the agency holds; the harms that could result from possible security breaches; and the likelihood that particular kinds of breaches might occur. "Risk is a function of the likelihood of a given threat-source's exercising a potential vulnerability, and the resulting impact of that adverse event on the organization." NIST Special Publication 800-30 at 8 (discussed at 394 F. Supp. 2d at 179-82).

3. This statutory and regulatory structure reflects the fundamental realities of information security. Because the effectiveness of computers and computer systems depends on their ability to communicate with each other, security concerns must be evaluated and addressed on an agencywide, and ultimately on a governmentwide, basis. See 44 U.S.C. §§ 3543, 3544. Because all security is relative, and because resources are finite, that evaluation depends on a series of risk determinations and judgments as to how best to allocate limited funds. And because the security decisions of each agency are of concern to the government as a whole, agency heads do not have final authority to approve security plans. That responsibility is placed in OMB, which coordinates security efforts governmentwide. See 44 U.S.C. § 3543.

Neither the FISMA, nor any guidance from NIST or OMB, dictates that computers should be disconnected when potential security threats are discovered. Nor do these provisions suggest that wholesale dismantling of computer communications would ever be appropriate. In applying FISMA standards, decisionmakers

would undertake such action only after weighing the costs to the public and the government that would result from such disruption.

Perhaps unsurprisingly, Dr. Ron Ross, a NIST scientist and principal author of relevant NIST standards, testified that, in his seven years at NIST, those standards have never led to the denial of approval to operate a computer system due to security concerns. Dr. Ross was asked, "[n]ow, in your experience there at the FISMA implementation team, generally how often in the federal government is a system denied the authority to operate?" Ross, 7/5/05 AM at 40. When Dr. Ross declared that "I've never seen any in my experience," the district court interjected, "[n]o matter how the risk assessment went, you've never seen anything ever shut off?" Ibid. Dr. Ross informed the court that this was, indeed, correct. Id. at 40-41.

Similarly, OMB guidance addresses the issue of service interruption only as a threat to security. See OMB Circular A-130, App. III, § B(a)(2)(e) ("When automated support is not available, many of the functions of the organization will effectively cease. Therefore, it is important to take cost-effective steps to manage any disruption of service."). OMB guidance specifically stresses that "[m]anual procedures are generally not a viable backup option." Ibid. OMB's concern is reflected in the FISMA itself, which does not require disconnections but rather requires that an agency's information security program include "plans and procedures to ensure

continuity of operations for information systems that support the operations and assets of the agency." 44 U.S.C. § 3544(b)(8).

**B. Governmentwide Experience Under The FISMA  
Underscores The Difficulty And Complexity Of  
The Security Problems Faced By Agencies And  
OMB.**

Since the enactment of FISMA, a subcommittee of the House Committee on Government Reform has given each executive agency an annual computer security grade based on its overall progress regarding the FISMA's security management requirements. In 2003, eight cabinet departments received an "F" on this congressional report card, including the Departments of the Interior, Justice, State, Homeland Security, Energy, Health and Human Services, Housing and Urban Development, and Agriculture. Docket #2418. Five of these eight agencies again received an "F" grade in 2004, with Interior obtaining a C+, Justice a B-, and State a D+. Docket #2933 at 7 n.11; 2004 Subcommittee Scorecard, available at <http://reform.house.gov/UploadedFiles/2004%20Computer%20Security%20Report%20card%202%20years.pdf>. (Two additional agencies, Commerce and the Veterans Administration, fell from a "C" to an "F" from 2003 to 2004, see ibid.)

In its 2004 scorecard, the Committee on Government Reform thus rated Interior higher than several cabinet agencies, including Homeland Security. As the examples of Commerce and the VA indicate, an agency's "grade" may fall as well as rise. The point is not Interior's relative rating in a given year. Rather, the significance of this scoring process is to highlight the

difficulties faced by agencies government-wide. Indeed, in a July 2005 report issued by the Government Accountability Office ("GAO"), the Comptroller General found that "[p]ervasive weaknesses exist in almost all areas of information security controls at 24 major agencies, threatening the integrity, confidentiality, and availability of information and information systems." PX581 at 2. "As a result," the Comptroller General continued, "federal operations and assets are at increased risk of fraud, misuse, and destruction. In addition, these weaknesses place financial data at risk of unauthorized modification or destruction, sensitive information at risk of inappropriate disclosure, and critical operations at risk of disruption." Ibid.

To take one example, the Department of Defense ("DOD"), which houses systems at least as critical as Interior's, is in no way immune from these government-wide problems. In its July 2005 analysis, the GAO listed DOD, along with 13 other agencies, including Interior, as having weaknesses in each of five basic IT security areas. PX581 at 9. A 2004 report by DOD's Inspector General reflects the same types of concerns voiced by other IG's (including Interior's Inspector General); the report concluded that "[t]he DOD warfighting capability and the security of its information infrastructure are at great risk from attacks by foreign intelligence organizations, cyber terrorists, and the incompetence of some of its own users." Information Technology, DOD FY2004 Implementation of FISMA for IT Training and Awareness



(12/17/04), at 21, available at <http://www.dodig.osd.mil/Audit/reports/FY05/05-025.pdf>.

The private sector, of course, faces the same challenges and has been repeatedly victimized by major hacking incidents. See Smith, 7/13/05 AM at 37. Indeed, even as the 59-day hearing in this case was underway, the national media reported major computer security breaches at financial institutions and universities across the country, including one incident in which a hacker accessed 40 million credit card numbers.<sup>1</sup>

None of this criticism suggests that the government is in any respect neglecting IT security, or that it has failed to make substantial progress. To the contrary, as the GAO declared, "[o]verall, the government is making progress in its implementation of the provisions of FISMA." PX581 at 2. The point is simply that computer security poses enormous and novel challenges. OMB, the Inspector Generals, the GAO and congressional oversight committees foster improvements by studying vulnerabilities and evaluating responses on an ongoing

---

<sup>1</sup> See 40 Million Cards May Be Affected By Breach, Washington Post, 6/19/05, at A21; see also, e.g., Associated Press, Computer Breach at U. of Connecticut, N.Y. Times, 6/25/05, at C13 (computer hacker gained access to the names, birth dates, and SSNs of 72,000 university students and employees); Hacker Accesses USC Files, L.A. Times, 7/9/05, at B3 (hacker accessed personal information regarding 270,000 current and former applicants to University of Southern California). For listings of IT hacking incidents in 2005, see, e.g., Privacy Rights Clearinghouse, A Chronology of Data Breaches Reported Since the ChoicePoint Incident, <http://www.privacyrights.org/ar/ChronDataBreaches.htm>; Identity Theft Resource Center, <http://www.idtheftcenter.org/breaches.pdf>.

basis. As a result, GAO observed, "[t]he government is progressing in its implementation of the information security management requirements of FISMA," but it is equally clear that "challenges remain." Id. at 14.

**C. The Record Provides No Basis For Continuing Judicial Intervention In Computer Security.**

**1. A Court Should Properly Defer To Decisions Taken As Part Of The FISMA Scheme.**

As the previous discussion indicates, in responding to everchanging threats to information security, the Executive Branch must employ both technical expertise and institutional judgment to prioritize risks and utilize limited resources in a cost-effective manner. The FISMA, as well as NIST and OMB guidance, stress these points repeatedly. For good reasons, they do not establish substantive security criteria, instead requiring accountable officials to evaluate and expressly accept risks. Ultimately, moreover, any single agency's security program reflects not only that agency's judgment, but the overall FISMA review process, which provides for independent evaluations to be submitted to congressional oversight committees and also to OMB, which is empowered to approve or disapprove agency security programs.

The judicial review principles stressed by this Court in its November 2005 decision vacating the re-issued accounting injunction apply with at least equal force to a review of information security arrangements subject to FISMA. It is incontrovertible that "[t]he choices at issue required both

subject-matter expertise and judgment about the allocation of scarce resources, classic reasons for deference to administrators." 428 F.3d at 1076 (citing Heckler v. Chaney, 470 U.S. 821 (1985), and Steel Manufacturers Ass'n v. EPA, 27 F.3d 642 (D.C. Cir. 1994)). The need for deference is underscored by the statutory procedures for ongoing evaluation within the Executive Branch and by the terms of a statute explicitly vesting in Executive officials the responsibility for discretionary decisions based on risk and cost assessments. See In re Barr Laboratories, Inc., 930 F.2d 72, 76 (D.C. Cir. 1991) ("we have no basis for reordering agency priorities. The agency is in a unique - and authoritative - position to view its projects as a whole, estimate the prospects for each, and allocate its resources in the optimal way"); Central & Southern Motor Freight Tariff Ass'n v. United States, 757 F.2d 301, 321-22 (D.C. Cir. 1985) ("[d]eference is particularly appropriate when" agency discretion "necessarily involves the administrative weighing of the costs and benefits").

As this Court has made clear, it is not for a "supervising court, rather than the agency, to work out compliance with the broad statutory mandate," a regime that would improperly "inject[] the judge into day-to-day agency management." 392 F.3d at 472 (quoting Southern Utah, 542 U.S. at 66-67); see also ibid. (warning against "'judicial entanglement in abstract policy disagreements which courts lack both expertise and information to resolve'").

2. **No Basis Exists For Setting Aside Executive Branch Security Decisions And Substituting Judicial Controls.**
  - a. **The Record Demonstrates Unstinting Commitment To The FISMA Process And Substantial Progress In IT Security.**

The record provides no basis for setting aside Executive Branch security decisions and substituting judicial controls.

The record leaves no doubt as to the agency's commitment to improvement or as to its actual progress. As the district court noted, Interior has invested over \$100 million in IT security in a three-year period. 394 F. Supp. 2d at 267-68. The court was obliged to acknowledge that "[t]here can be no doubt that Interior has made substantial progress in implementing a comprehensive departmental IT security program in a very short time," *id.* at 249, and it even observed that "Interior's progress in a period of five years is laudable," *id.* at 272. See also, e.g., *id.* at 274 ("Interior is currently devoting substantial time and resources to IT security").

The district court's praise underscores Interior's recent accomplishments in improving the security of trust-related information. Testimony at trial established, for example, that the IG's hacking contractor was unsuccessful in its attempts to penetrate the computer systems of MMS, which every month receives, processes, and disburses hundreds of millions of dollars in royalty and lease payments. *Id.* at 213-14. Similarly, with respect to the IG's efforts to hack into the BIA's systems from a simulated internet connection, the

contractor's report remarked: "If this environment were accessible from the Internet, it would be an extremely small footprint for such a large organization." Id. at 210. And even in instances where the IG's professionals were able to exploit potential weaknesses in Interior's computer security, they "noted the presence of several kinds of security controls that [were] in keeping with the 'best practices' of the IT security community," id. at 209, and system elements "that were compromised ... exhibited a number of good security practices such as up to date security patches, security monitoring software, and strong password policies that eliminate many common vulnerabilities and reduced the impact of identified vulnerabilities," id. at 213 (quoting contractor report); see also id. at 219 (same).

Interior's progress reflects an unstinting commitment to making the FISMA process effective. The IG's penetration testing that gave rise to plaintiffs' request for an injunction was undertaken at Interior's direct invitation and was made possible by Interior's offer to fund that testing in order to advance its security efforts. As the IG testified, he was contacted in 2003 by James Cason, the Associate Deputy Secretary of the Interior, who "said that he'd like to have some independent [IT security] testing done" sometime in "the late fall of 2003." 394 F. Supp. 2d at 201-02 (quoting Devaney, 5/20/05 AM at 35-36). Mr. Cason explained "that he was at a point where he wanted to begin to see if the systems would withstand penetration, and asked me if I would be willing to be the independent tester if they gave us

some money to do that to hire a contractor." Id. at 202 (quoting Devaney, 5/20/05 AM at 36). Prior to that time, "Interior's IT security program had simply not advanced far enough for penetration testing to be a useful evaluation tool." Id. at 200.

The IG testified that Interior's initiative was vital to his ability to undertake penetration testing. Interior's offer, the IG declared, allowed him "to jump start that program that I was trying desperately to find funds" to implement. Id. at 202 (quoting Devaney, 5/20/05 AM at 37). Interior's offer was memorialized in a Memorandum of Understanding with the IG by which Interior agreed to fund the penetration testing. PX1; see also 394 F. Supp. 2d at 185-86 (noting IG's testimony that Secretary Norton had never exercised her authority to lower the IG budget). As Interior's Chief Information Officer ("CIO") emphasized in his testimony, the essential purpose of the penetration testing, which, as noted, the Department itself initiated, was to expose potential vulnerabilities thereby enabling their remediation. See Tipton, 7/26/05 PM at 76, 87-88.

**b. The Problems Cited By The District Court  
Provide No Basis For Judicial Intervention.**

The evidence at trial thus suggested neither a lack of progress nor a failure to commit to progress. The precise strengths and weaknesses of Interior's evolving security program may be debated, but the trial evidence provided no basis for concluding that judicial action of any kind is necessary to

ensure that the FISMA process operates in the manner that Congress intended.

The IG's penetration testing, undertaken at Interior's behest, forms part of an internal and ongoing Executive Branch process and provides no ground for judicial involvement. The IG noted that Congress had recently given Interior a C+ computer security grade, "I think recognizing the progress that has been made." However, "this penetration testing in my mind has taken that grade back to F." Devaney, 5/20/05 PM at 59. As the IG testified, it is not his role to assign a grade, id. at 60, and he acknowledged that neither he nor his staff was prepared to offer any opinion on the security of Interior's computer networks generally, see Devaney, 5/20/05 AM at 85-89, or of its trust data in particular, see id. at 88. Indeed, the IG specifically cautioned against drawing conclusions about Interior's information security from the penetration testing results. Devaney, 5/20/05 AM at 87; accord Miles, 5/18/05 PM at 100 (testimony of IG's hacking contractor noting that penetration testing did not permit meaningful appraisal of Interior's overall security posture).<sup>2</sup> In any event, as discussed above, the

---

<sup>2</sup> Asked whether he could offer the court any representations concerning the security of trust-related data on Interior's computer networks, Inspector General Devaney testified:

I think the only representation I can make is the snapshots that we took here. We came in at a given time and penetrated the system in a certain way. If we were to come back the day after, or if we had done it  
(continued...)

relative grades accorded by congressional oversight committees are significant chiefly because they reveal the magnitude of the problems presented government-wide, and preclude any inference that problems faced at Interior result from a lack of commitment or unique difficulties in developing effective responses.

Indeed, the testimony made clear that vulnerabilities found at Interior were not in any sense unusual among government agencies. To the contrary, Roger Mahach, a member of the IG's staff, testified that "I don't think any government program, whether it's at the Department of Interior, the EPA, or the Food and Drug Administration or Homeland Security can withstand this type of scrutiny." Mahach, 6/10/05 PM at 80.

Similarly, an employee of the firm retained by the IG to hack into Interior's computers testified that it is commonplace for testing of this kind to result in successful penetration. Scott Miles, who personally conducted much of the hacking in question, estimated that the kind of penetration testing conducted by his firm on behalf of government and private clients is generally successful about 75 percent of the time. Miles, 5/18/05 PM at 62; see Brass, 5/09/05 PM at 85 (same).

---

<sup>2</sup>(...continued)

the day before, we might not have gotten in. We might have through a more - we might have tried to get in and been rebuffed. The fact that we got into two of these bureaus and were able to do what we did gives me great concern, but I can't say that tomorrow, if penetration testing was done, that we would be successful.

Devaney, 5/20/05 AM at 87.



Although the district court referred broadly to "fundamental systemic problems inherent in the structure of Interior's IT environment," 394 F. Supp. 2d at 271, it did not conclude that the problems faced by Interior were different in kind or scope than those at other agencies. Many of the issues that the court found troubling involved perceived bureaucratic shortcomings of the type endemic to all large organizations. See, e.g., id. at 194 (failure to place copies of risk-assessment documentation in all field offices); id. at 196-97 (inadequate "plan of action and milestone" (POA&M) documentation); id. at 197 (failure to update POA&M documentation in a timely fashion).

More fundamentally, when an agency is fully cooperating in the FISMA scheme and is making substantial progress, no apparent basis exists for a court to intrude into the operations of the statutory scheme. Nor, in these circumstances, is it at all apparent what relief a court could order consistent with the statute's emphasis on cost-effective risk assessment by agency officials, with independent evaluation by the IG, close congressional oversight, and ultimate review authority vested in OMB.

**3. No Evidence Exists Of Past Or Imminent Threats To Accountholder Security That Would Warrant Judicial Intervention.**

As the previous discussion indicates, protection of IITD cannot be considered in isolation from the agencywide security program. Even if a legal basis existed for questioning the precise protections accorded to IITD within that program (and

even assuming that such an inquiry were feasible), the record provides no basis whatsoever for inferring that IITD is at any imminent risk of corruption. Indeed, no evidence exists of even one instance of unauthorized computer tampering with the IIM account of any member of the plaintiff class.

When IG auditor Diann Sandy (praised by the court for telling the "unvarnished truth," 394 F. Supp. 2d at 186 n.11) was asked whether "in the 20-plus years that you've been an auditor with the IG's office," she had "ever heard of an instan[ce] in which someone manipulated data within Interior's systems and arranged to have an Individual Indian Trust beneficiary's payment sent to someone other than the intended Trust beneficiary," she testified "[n]ot to my knowledge." Sandy, 6/6/05 PM at 83.

Moreover, as the trial testimony underscored, the ability of retained security experts to gain access to a computer system does not indicate that other individuals, lacking similar expertise and immunity from criminal prosecution, see 18 U.S.C. § 1030, would easily enjoy similar success. As noted by Mr. Mahach, an IG employee with substantial involvement in the penetration testing of Interior, "[t]he success of the Office of Inspector General's penetration testing is not ... due to trivial weaknesses that allow for easy, automated exploitation by unskilled hackers. Commonly used and readily available automated tools used by [unskilled hackers] would not find the type of weaknesses we have been able to exploit." PX41. Similarly, authorized hackers can focus their efforts on gaining entry

without investing comparable time and resources to ensuring that their efforts will not be traced. Nor did the evidence explain why unauthorized hackers would be motivated to risk potentially severe criminal sanctions to tamper with IIM accounts, see, e.g., Brass, 5/09/05 AM at 64 (noting that malicious hackers seeking to break into government computer files face "a long stay in Leavenworth").

**4. The District Court's Belief That IITD Should Be "Segregated" Reflects a Fundamental Misunderstanding Of Computer Systems And Limitations Of Judicial Expertise.**

Although the injunction does not specify how the district court would exercise its ongoing control of Interior's computers, its decision suggests that "the most immediate, commonsense step to securi[ng] electronic trust data" would be the segregation of IITD onto systems isolated from Interior's general network. 394 F. Supp. 2d at 261; see also id. at 258, 271. During the 59-day hearing, the district court repeatedly interrupted the testimony to ask witnesses why, in their view, Interior had failed to undertake the complete segregation of trust data. See, e.g., Tr. 5/12/05 PM at 34-35 (Mahach); Tr. 6/30/05 PM at 70-71 (Brown).<sup>3</sup>

---

<sup>3</sup> Typical was this interjection during plaintiffs' direct examination of Roger Mahach:

THE COURT: I can't help interrupting. I'm burning with one question that I have never understood.... Why after all the problems in 2001 with the trust records and this Court's concerns, why has the trust record never been separated out from the other systems so we didn't have to put the whole department at risk and we could have just had the trust records on one  
(continued...)

And in its opinion accompanying the injunction, the district court expressed disapproval over what it perceived as "Interior's continuing inability to ... segregat[e] IITD on secure servers separate from Interior's accessible IT networks and systems." 394 F. Supp. 2d at 261.

The district court's focus on "segregation" as the appropriate security strategy for IITD is symptomatic of the flaws in its analysis and underscores why judges do not properly assume administrative authority for safeguarding the government's computer networks. The court's evident belief that Interior "could have just had the trust records on one system," Tr. 5/12/05 PM at 34-35, is at odds with the court's own recognition that IITD "permeates Interior's IT environment fairly completely." 394 F. Supp. 2d at 258. Nothing in the record suggests that Interior could identify, aggregate, and organize into a single isolated system all of its electronic information that "evidences, embodies, refers to, or relates to – directly or indirectly and generally or specifically – a Federal Record that reflects the existence of Individual Indian Trust Assets," *id.* at 277 (injunction's definition of Individual Indian Trust Data).

As one government witness testified, a true "segregation" program would arguably require the wholesale duplication of major

---

<sup>3</sup>(...continued)  
system? .... [I]t's been four years. Why hasn't that been done?

Tr. 5/12/05 PM at 34-35.

Interior computer networks, and of the human and capital resources necessary to operate those networks. See Brown, 6/30/05 PM at 70-71, 76-77. Even then, the witness noted, segregation might not appreciably improve the security of trust data, because duplication of existing networks would merely duplicate many existing vulnerabilities. Ibid. Moreover, even if such an undertaking were thought desirable, the costs would be prohibitive. As the district court itself acknowledged, one of the reasons Interior has not pursued a strategy of complete segregation is "because the resources that such an effort would require are simply not available." 394 F. Supp. 2d at 258; see Cason, 7/18/05 PM at 75-77 (noting resource constraints).

The problems inherent in judicial second-guessing of complex security decisions are evident throughout the court's opinion. For example, the court disagreed with the agency's choice of spending priorities, noting that while Interior had sponsored the testing of its network security, it had not given the same weight to security testing of agency employees and third-party contractors, thus wrongly failing to make such testing "a priority within the departmental IT security program." 394 F. Supp. 2d at 256. This is precisely the type of judgment that an agency must be allowed to make, and judicial intervention would be inappropriate even if the record demonstrated actual problems with IITD security due to employees and contractors. In fact, the court cited no such evidence.

Similarly, the court criticized Interior at length because it believed that the language of contracts with third-party contractors did not mandate adequate testing of the contractors' systems. See id. at 256-57. In this manner, the court not only undertook to second-guess security judgments as to what testing might be required, but also assumed authority to judge the level of explicit detail to be included in Interior's contractual arrangements. The impropriety of such judicial micromanagement is further underscored by the absence of citation to evidence that any contractor system has, in fact, placed any data - much less IITD - at an unacceptable risk of corruption or loss.

In short, the court's analysis highlights its failure to appreciate that Interior's discretion in implementing the FISMA process requires "both subject-matter expertise and judgment about the allocation of scarce resources." 428 F.3d at 1076.

**D. In Assuming Control Of Interior Computer Systems, The District Court Replicated The Errors Underlying Its Previous Structural Injunctions.**

As we have shown, neither the governing statutory and regulatory scheme nor the record at trial provides any basis for setting aside any aspect of Interior's information security program. Accordingly, the matter of information security is properly remanded to the Executive Branch to be addressed by Interior, its Inspector General's Office, and OMB, which are responsible to Congress for the effective operation of the FISMA scheme.

The court would thus have erred even if it had simply remanded with instructions to alter one or more security priorities. The full extent of the court's improper arrogation of Executive Branch responsibilities is thrown into relief by its decision to appoint itself the arbiter of future compliance with unidentified standards, and, for an indefinite period, to require massive disconnections as an alternative agency security program. In so doing, the court not only departed from this Court's directive to accord substantial deference to complex agency judgments, but also departed from other crucial strictures emphasized by this Court in reversing previous structural injunctions.

1. The district court wrongly believed that it was licensed to undertake control of information security programs because of the fiduciary relationship between Interior and IIM accountholders. The court emphasized that judicial intervention was appropriate notwithstanding "the substantial progress that has been made," because, in the court's view, "Interior has not properly emphasized IITD in its IT security efforts." 394 F. Supp. 2d at 272. The court explained that because IIM accountholders are trust beneficiaries, the FISMA scheme could not be considered controlling. The court declared that "[t]o be sure, certification and accreditation is the standard with which Interior must comply to adhere to OMB's guidance for complying with FISMA." Id. at 264. But "the Court cannot accept certification and accreditation alone as sufficient to show that

Interior's IT systems are presently adequately secure to comply with Interior's fiduciary obligations as Trustee-delegate for the IIM trust." Ibid. On this basis, the court explained that it was appropriate to order a restructuring of security efforts even though "[p]riorities will likely have to be shuffled, resources will likely have to be redirected[.]" Id. at 275.

As this Court made clear in vacating the first structural injunction, the trust relationship between the government and IIM accountholders does not vitiate normal limits on judicial review. This Court explained that a judicial takeover of agency responsibilities is not only inconsistent with general principles of judicial review, 392 F.3d at 471-78, but is without foundation in general principles of fiduciary law. This Court noted that "private trustees, even though held to high fiduciary standards, are generally free of direct judicial control over their methods of implementing these duties, and trustee choices of methods are reviewable only 'to prevent an abuse by the trustee of his discretion.'" 392 F.3d at 473 (citing Restatement (Second) of Trusts §§ 186-87).<sup>4</sup> Moreover, as this Court observed, in private trusts, the costs of trust administration are met from the trust itself, 392 F.3d at 473, and decisions necessarily incorporate a cost-benefit analysis.

---

<sup>4</sup> Thus, as Professor Langbein explained earlier in this litigation, under common law principles, a court would be reluctant to interfere with the manner in which a trustee seeks to implement its duties, particularly when the trustee must determine how best to use limited funds. See Langbein, 6/3/03 PM at 74-76, 78-79; Langbein, 6/3/03 AM at 33-34, 39, 67-68.



Thus, in vacating the re-issued accounting injunction, this Court explicitly held that the district court had erred when it "invoked the common law of trusts and quite bluntly treated the character of the accounting as its domain." 428 F.3d at 1076. In so doing, the court had "erroneously displaced Interior as the actor with primary responsibility for 'work[ing] out compliance with the broad statutory mandate.'" Ibid. (quoting Southern Utah, 542 U.S. at 66-67).

2. As in its previous structural injunctions, the district court disregarded this Court's admonition that a court is empowered only to compel an agency "'take action upon a matter, without directing how it shall act,'" 392 F.3d at 475 (citation omitted), and improperly established an ongoing regime that will "inject[] the judge into day-to-day agency management," id. at 472. The court in effect installed its own version of an information security program, one that requires wholesale computer disconnections. Future changes to that program will be made at the court's sole discretion following extended adversary proceedings in which Interior will carry the burden of persuasion. 394 F. Supp. 2d at 279. The injunction is flatly at odds with this Court's warning against "'judicial entanglement in abstract policy disagreements which courts lack both expertise and information to resolve,'" and against "'pervasive oversight by federal courts over the manner and pace of agency compliance with [broad] congressional directives,'" 392 F.3d at 472 (quoting Southern Utah, 542 U.S. at 64).

Of course, the district court's order did not rest on a purported failure to comply with any particular congressional directive. To the contrary, it is the court's alternative security regime that cannot be reconciled with the statute. As discussed above, the FISMA itself neither mandates agency computer disconnections nor suggests any circumstance in which sweeping disconnections are appropriate. Evidence at trial indicated that no federal agency had ever been denied authority to operate a computer system under the FISMA and NIST standards. Ross, 7/5/05 AM at 40. If the Executive Branch, in the course of fulfilling its FISMA responsibilities, were to contemplate the option of wholesale computer disconnections, it would be required to weigh the magnitude and likelihood of the harm to be avoided against the costs in terms of money and degradation of its ability to serve the public. It is difficult to posit what extraordinary circumstance might cause the Executive Branch to engage in widespread, indefinite, external and internal computer disconnections. Nothing in the FISMA could plausibly be construed to mandate such disconnections here.

More fundamentally, a statute that requires responsible Executive Branch officials to evaluate and accept risks is incompatible with judicial revision of security priorities. The extended trial provided no basis for such intervention, and the provisions of the injunction further depart from principles repeatedly emphasized by this Court.

## **II. The Injunction Cannot Be Reconciled With Basic Principles of Equity.**

As we have shown, the injunction is based on fundamental error and cannot be sustained. However, even if the order were reviewed solely in terms of guiding principles of equity, reversal would be required.

The district court has required a Cabinet department to disassemble much of its electronic communications network, both with respect to the public and other federal agencies, and with respect to its own, internal communications. The extraordinary history of this litigation perhaps obscures the utterly remarkable nature of such a ruling. If a court required the Social Security Administration to sever its internet links with the public, the outcry would be immediate. Likewise, it is scarcely conceivable that a court would preclude the Secretary of State or the Secretary of Homeland Security from communicating electronically within large segments of their own agencies. An order inflicting this type of damage on the Department of the Interior is no more supportable.

### **A. The Injunction Is In No Meaningful Way "Preliminary."**

As an initial matter, although the district court styled its order a "preliminary" injunction, the appellation is plainly a misnomer. The injunction is not "preliminary" to any pending "merits" dispute. The injunction establishes an alternative information security plan that will remain in effect until Interior carries a burden of persuading the court, in further

adversary proceedings, that individual computer systems should be reconnected. An injunction that remains in effect indefinitely and shifts the burden of persuasion to the nonmoving party does not remotely resemble a true preliminary injunction, the purpose of which is "merely to preserve the relative positions of the parties until a trial on the merits can be held." University of Texas v. Camenisch, 451 U.S. 390, 395 (1981); see Washington Metropolitan Area Transit Comm'n v. Holiday Tours, Inc., 559 F.2d 841, 844 (D.C. Cir. 1977).

**B. An Injunction Must Take Into Account The Public Interest And Be Tailored To Limit Its Adverse Impact On The Defendant.**

Apart from the absence of legal authority, a fundamental reason that courts do not cripple the communications of Executive Branch agencies is the bedrock principle that a court must consider the public interest in fashioning equitable relief. As this Court has long made clear, injunctive relief must "eventuate from a careful consideration of all important factors of relevance, not the least of which is the public interest." Udall v. D.C. Transit System, Inc., 404 F.2d 1358, 1360 (D.C. Cir. 1968) (per curiam); see Weinberger v. Romero-Barcelo, 456 U.S. 305, 312-13 (1982).

It is difficult to posit any circumstance in which the public interest could be harmonized with an order destroying significant parts of a cabinet agency's internal communications structure as well as its ability to communicate with the public that it serves. The district court made no serious attempt to

explain how the harms resulting from its order are compatible with the public interest.

To list the specific harms flowing from the injunction is to understate its impact. The Court can readily apprehend the effect of an order requiring the federal judiciary to dismantle its internet connections and to disconnect individual computers from other computers. The impact of such an order on a massive executive agency is no less significant. The injunction would have a devastating effect on even the most routine communications within and among the Interior bureaus, components, and field offices that handle trust-related information.

The Department of the Interior is a cabinet agency with an annual budget of \$11 billion and approximately 70,000 employees. Declaration of W. Hord Tipton (3/22/04) at 1. The Department manages one out of every five acres of land in the United States; provides the resources for nearly one-third of the nation's energy; provides water to 31 million people through 900 dams and reservoirs; receives over 450 million visits each year to the parks and public lands it manages; and implements hundreds of statutorily-mandated programs. Ibid. In addition, the Department provides a variety of critical services on which other federal agencies rely. Ibid.

To meet its responsibilities, the Department manages a portfolio of approximately \$1 billion of information technology, including approximately 100,000 computers. Ibid. Even if the court had required severance only of internet connections and had

not addressed internal connections, the injunction would undermine the agency's mission and its ability to serve individual Indians and Tribes, other federal agencies, and the public in general. As Secretary Norton explained in her declaration filed in connection with the district court's March 2004 disconnection order, "Internet communication is not merely a useful tool - it is essential to much of what we do."

Declaration of Gale A. Norton (3/22/04) at 1.

The internet disconnection component of the injunction would frustrate the ability of the Minerals Management Service to receive, process, and disburse over \$500 million in mineral revenues on Federal and Indian leased lands paid by about 2,000 companies each month. MMS accomplishes this mission through delivery of reporting, accounting, and financial services. Tipton Decl. 7. As explained by Interior's CIO, "[a]ll such functions are heavily reliant on automated systems and access to the internet." Ibid.; see Cason, 7/18/05 AM at 38 ("the Minerals Management Service relies upon the Internet heavily to collect the information necessary to process rents, royalties, and bonuses owed to the federal government, including those for Indians").

Minerals revenues are a major source of income for forty-one Indian Tribes; approximately 20,000 individual Indian minerals owners; the federal government; and thirty-eight states. The court's internet disconnection mandate would thus prevent or hinder MMS from being able to make timely monthly disbursements

of over \$500 million in mineral revenues to States, Indians, and Treasury accounts. Tipton Decl. 7. As MMS's Deputy CIO testified, "if we have to shut down from the Internet, the oil and gas companies cannot put their production data into the system, and, therefore, we can't collect the royalties and put that money into the Treasury and, therefore, royalty checks are not paid out to all the allottees." Ekholm, 7/8/05 AM at 12; see Smith, 7/12/05 PM at 56-57 (same).

Other core aspects of Interior's operations that would be affected by an internet shutdown include the Department's personnel, procurement and financial management functions. See Tipton Decl. 3-7. As the record shows, Interior's National Business Center ("NBC") hosts major computer systems that "pay[] approximately 250,000 federal employees [across the government], as well as providing financial management [services] for approximately 30 or 40 different federal organizations, including the Department of Interior." McWhinney, 7/21/05 PM at 4; see Haycock, 7/14/05 PM at 73 ("we have 37 federal clients that we process their personnel actions and pay them.... All of that is computer based."). Impairing the networking capability of these systems "would [thus] have a severe impact on financial management for large portions of the federal government." McWhinney, 7/21/05 PM at 4.

This injunction does not only require new internet disconnections and preclude restoration of connections previously severed. The injunction also requires an internal, intranet

disconnection, 394 F. Supp. 2d at 277-78. Components such as MMS would have to sever their internet connections and also sever their connections to all other offices and bureaus within the Department. Components such as the Bureau of Indian Affairs and the Office of Special Trustee, which had not yet regained internet access, would not be permitted to reconnect and would lose their ability to communicate with other components. To make the calamity complete, affected systems must also dismantle internally within each office and bureau. Thus, every BIA computer must be disconnected from every other BIA computer, every OST computer must be disconnected from every other OST computer, and so on. Ibid. In effect, each affected computer would be transformed into a stand-alone unit isolated from every other computer and computer device in the Interior Department. Ibid.; Declaration of James E. Cason (10/27/05) at 4. As a result, users of the disconnected computers would be deprived of even the most rudimentary e-mail capacity. Implementing the court's order would also result in the loss of basic telephone service for Interior employees who depend on "Voice Over Internet Protocol" (VOIP) telephone systems. Ekholm, 7/8/05 AM at 14 ("we would have to turn off those phone systems"). VOIP is expressly included in the order's definition of "Information Technology System" to which the court's injunction applies (as are hand-held wireless "Blackberry" devices, which provide both telephone and e-mail services). 394 F. Supp. 2d at 276-77.



The court's order would have a particularly harsh impact on services to Indians. Among its many responsibilities, BIA distributes social services payments for individual Indians. To perform that function, it relies upon the automated Social Services Assistance System ("SSAS"). The SSAS system, used by BIA and Tribes, contains financial data used to generate public assistance checks and maintain individuals' files. As the record makes clear, "[i]f that system is shut down, those welfare payments will stop." McWhinney, 7/21/05 PM at 5.

These and other consequences of the injunction are in no way alleviated by its provision, proposed by plaintiffs, that Interior may, after providing written notice to the court and plaintiffs' counsel, "reconnect, for specified periods not to exceed five (5) business days per month, any Information Technology System that Houses or provides Access to Individual Indian Trust Data, for the purpose of receiving and distributing trust funds, or for the purpose of conducting other necessary financial transactions." 394 F. Supp. 2d at 278.

The apparent premise of this provision is that complex, interconnected computer systems can repeatedly be turned on and off without impact on their functions. It is wholly unclear why the district court would embrace such a mistaken assumption. Like other aspects of its order, this provision highlights the limits of judicial competence to superintend complex information technologies. As is the case with analogous systems in the government and private sector, the computer systems at issue

depend on an ongoing input and exchange of massive amounts of information that cannot be arbitrarily compressed into brief, intermittent periods in which they may receive, process and forward critical data. See Cason Decl. 3, 12-14.

Moreover, this provision is hardly calculated to deal with the asserted threats to IITD. If that data were (contrary to fact) facing imminent, irreparable compromise, it is unclear why hackers could not inflict that harm during the five available days of operations. Indeed, because Interior would have no ability to download "patches" from the internet to guard against new security hazards, the systems would be even more vulnerable when returned to operation. See Tipton Decl. 8; Ekholm, 7/8/05 AM at 11 ("that makes you more vulnerable in many ways because you cannot patch your systems in a timely fashion").

More generally, the negative impact of repeated dismantlings of computer operations should be self-evident. As OMB guidance points out, to guard against the effect of service interruptions, "[a]gency plans should assure that there is an ability to recover and provide service sufficient to meet the minimal needs of users of the system. Manual procedures are generally not a viable back-up option. When automated support is not available, many of the functions of the organization will effectively cease. Therefore, it is important to take cost-effective steps to manage any disruption of service." OMB Circular A-130, App. III, § B(a)(2)(e). That a court would deliberately inflict this type of damage on an agency beggars belief.

The court opined that "BIA and OST have been disconnected from the Internet for years, yet still manage to carry out their Indian-related missions. Solutions implemented to allow these bureaus to function without access to the Internet should be fairly easily adapted and exported to other bureaus and offices." 394 F. Supp. 2d at 275. This statement is wrong in every respect. First, Interior's quarterly reports repeatedly note that existing internet disconnections do indeed impair Interior's ability to carry out its missions, see, e.g., Report No. 21 at 9-10. Second, BIA, OST, and other components have relied in important respects on MMS's ability to gather production and royalty data through its internet connection, which would be severed by the order at issue, see McWhinney, 7/21/05 PM at 5; Cason Decl. 6-7. Finally, these components have at least been able to communicate internally and with other components. The present injunction, unlike the court's previous orders, would sever bureau-to-bureau and even computer-to-computer communications. 394 F. Supp. 2d at 277-78.

The district court was aware of "the ways in which the department's operations were disrupted by this Court's last disconnection order," and noted in passing "the effects that a loss of Internet connectivity would have on the department's ability to service its customers, many of whom are other governmental agencies." 394 F. Supp. 2d at 274. The court concluded, in effect, that the perceived interest in protecting IITD data constituted an overriding public interest that rendered

the impact of its ruling immaterial. No basis exists for singling out one public interest to the exclusion of all others and rendering all other public interests irrelevant.

**C. Plaintiffs Have Failed To Demonstrate That An Injunction Is Needed To Avoid Likely Irreparable Harm.**

The court's willingness to undermine a cabinet agency's communications is all the more remarkable because plaintiffs have failed to make a threshold showing of irreparable injury that would entitle them to any equitable relief at all (even setting aside the fatal problems with their position discussed at Point I and the impact on the public interest discussed at Point II.B).

No injunction may issue unless the movant demonstrates that "irreparable injury is 'likely' to occur." Wisconsin Gas Co. v. FERC, 758 F.2d 669, 674 (D.C. Cir. 1985). "Bare allegations of what is likely to occur are of no value since the court must decide whether the harm will in fact occur. The movant must provide proof that the harm has occurred in the past and is likely to occur again, or proof indicating that the harm is certain to occur in the near future." Ibid. (citation omitted, emphasis in original). This, plaintiffs failed to do.

As discussed, plaintiffs provided no evidence that even one class member has ever been harmed by unauthorized computer tampering. Moreover, an IG auditor testified that she had never, in more than 20 years, heard of an instance in which someone had manipulated data within Interior's systems and arranged to have a beneficiary's payment sent to someone else. Sandy, 6/6/05 PM at

83. Likewise, as shown, the fact that the Special Master and the IG, armed with resources, expertise, and immunity from prosecution, were able to penetrate some of Interior's systems does not demonstrate that other persons will have the motivation or means of doing so, let alone that irreparable harm to trust data would necessarily result, see Tipton, 7/26/05 PM at 70, 75. The evidence does not indicate that Interior systems are, on the whole, more vulnerable than those of other cabinet departments, and, indeed, the 2004 "scorecard" issued by the House Committee on Government Reform rated Interior higher than several other agencies. See Docket #2933 at 7 n.11.

Although the injunction will not avoid imminent irreparable harm to any class member, it will almost certainly operate to the detriment of many members of the plaintiff class who rely on Interior's services to at least the same extent as the public generally. Nor can class members take solace in the belief that the injunction, whatever hardships it may impose, at least advances their interest in obtaining timely and accurate account statements. As this Court has observed, although the failure to provide computer systems is not a breach of a legal duty, effective computer systems are essential to the agency's accounting processes. See 240 F.3d at 1106. Indeed, accounting activities, like much of Interior's work, are dependent on computer systems and electronic communications. See 391 F.3d at 257 ("maintaining adequate computer systems ... is critical to the completion of an adequate accounting"); see Haycock, 7/14/05

PM at 73 ("[w]e rely on computers to do almost everything we do"); Ekholm, 7/8/05 AM at 13-14 ("Pretty much all - nearly all of our operational functions are done in an automated fashion these days."). Thus, the effect of disabling computers and internal and external communications is to undermine those functions, including the performance of accounting activities that this lawsuit ostensibly seeks to accelerate.

With considerable understatement, the court acknowledged that compliance with its order would be "difficult," and that "[p]riorities will likely have to be shuffled, resources will likely have to be redirected[.]" 394 F. Supp. 2d at 275. The court's response was to declare that "[t]he relief granted today is not likely to prove popular in governmental circles. The Court is not, however, in the business of doing the popular thing, or the politically savvy thing. The Court must evaluate the evidence presented, and take the action that is warranted by that evidence." Id. at 274.

The court is quite right that its role is not to do the "popular" or "politically savvy thing." If it issues an injunction, however, it is obliged to operate within the traditional constraints on equitable authority. A court must consider the impact of its order on the public and on public services, and it may not redefine the public interest to include only one aspect of the interests of the plaintiff class. Similarly, an injunction can issue only if plaintiffs have carried their burden of demonstrating imminent irreparable harm,

and the court may not redefine irreparable harm to encompass harm that has never occurred in the past and is wholly conjectural in the future. These fatal failings would require reversal even apart from the equally fatal legal errors discussed in the first part of our argument.

**CONCLUSION**

This Court should vacate the October 20, 2005 injunction, which requires components of the Department of the Interior to disconnect their computers from internet and intragency access and also precludes some of those components from reestablishing internet access.

Respectfully submitted,

PETER D. KEISLER  
Assistant Attorney General

KENNETH L. WAINSTEIN  
United States Attorney

GREGORY G. KATSAS  
Deputy Assistant Attorney General

ROBERT E. KOPP  
MARK B. STERN  
THOMAS M. BONDY  
ALISA B. KLEIN  
MARK R. FREEMAN  
I. GLENN COHEN  
ISAAC J. LIDSKY

(202) 514-5089

Attorneys, Appellate Staff  
Civil Division, Room 7531  
Department of Justice  
950 Pennsylvania Ave., N.W.  
Washington, D.C. 20530-0001

*Thomas M. Bondy*  
*Alisa B. Klein*  
*Mark R. Freeman*  
*I. Glenn Cohen*  
*Isaac J. Lidsky*

JANUARY 2006

CERTIFICATE OF COMPLIANCE WITH RULE 32(a)(7)(c)  
OF THE FEDERAL RULES OF APPELLATE PROCEDURE

I hereby certify pursuant to Fed. R. App. P. 32(a)(7)(C)  
that the foregoing brief contains 13,989 words, according to the  
count of Corel WordPerfect 12.

  
THOMAS M. BONDY



**CERTIFICATE OF SERVICE**

I hereby certify that on this 11<sup>th</sup> day of January, 2006, I caused copies of the foregoing brief to be sent to the Court and to the following by hand delivery:

The Honorable Royce C. Lamberth  
United States District Court  
United States Courthouse  
Third and Constitution Ave., N.W.  
Washington, D.C. 20001

Keith M. Harper  
Native American Rights Fund  
1712 N Street, N.W.  
Washington, D.C. 20036-2976  
(202) 785-4166

G. William Austin  
Mark I. Levy  
Kilpatrick Stockton  
607 14th Street, N.W., Suite 900  
Washington, D.C. 20005  
(202) 508-5800

and to the following by federal express, overnight mail:

Elliott H. Levitas  
Law Office of Elliott H. Levitas  
1100 Peachtree Street  
Suite 2800  
Atlanta, GA 30309-4530  
(404) 815-6450

and to the following by regular, first-class mail:

Dennis Marc Gingold  
607 14th Street, N.W.  
Washington, D.C. 20005

Earl Old Person (pro se)  
Blackfeet Tribe  
P.O. Box 850  
Browning, MT 59417

  
THOMAS M. BONDY

## **STATUTORY ADDENDUM**

## ADDENDUM CONTENTS

Federal Information Security Management Act of 2002 (FISMA), 44 U.S.C. § 3541 <u>et seq.</u> . . . . .	1a
---	----

UNITED STATES CODE ANNOTATED  
United States Code Annotated Currentness  
TITLE 44. PUBLIC PRINTING AND DOCUMENTS  
Title 44. Public Printing and Documents (Refs & Annos)  
**CHAPTER 35--COORDINATION OF FEDERAL INFORMATION POLICY**  
Chapter 35. Coordination of Federal Information Policy (Refs & Annos)  
SUBCHAPTER III--INFORMATION SECURITY  
Subchapter III. Information Security (Refs & Annos)

**➔§ 3541. Purposes**

The purposes of this subchapter are to--

- (1) provide a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets;
- (2) recognize the highly networked nature of the current Federal computing environment and provide effective governmentwide management and oversight of the related information security risks, including coordination of information security efforts throughout the civilian, national security, and law enforcement communities;
- (3) provide for development and maintenance of minimum controls required to protect Federal information and information systems;
- (4) provide a mechanism for improved oversight of Federal agency information security programs;
- (5) acknowledge that commercially developed information security products offer advanced, dynamic, robust, and effective information security solutions, reflecting market solutions for the protection of critical information infrastructures important to the national defense and economic security of the nation that are designed, built, and operated by the private sector; and
- (6) recognize that the selection of specific technical hardware and software information security solutions should be left to individual agencies from among commercially developed products.

(Added Pub.L. 107-347, Title III, § 301(b)(1), Dec. 17, 2002, 116 Stat. 2946.)

→§ 3542. Definitions

**(a) In general.**--Except as provided under subsection (b), the definitions under section 3502 shall apply to this subchapter.

**(b) Additional definitions.**--As used in this subchapter:

**(1)** The term "information security" means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide--

**(A)** integrity, which means guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity;

**(B)** confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and

**(C)** availability, which means ensuring timely and reliable access to and use of information.

**(2)(A)** The term "national security system" means any information system (including any telecommunications system) used or operated by an agency or by a contractor of an agency, or other organization on behalf of an agency--

**(i)** the function, operation, or use of which--

**(I)** involves intelligence activities;

**(II)** involves cryptologic activities related to national security;

**(III)** involves command and control of military forces;

**(IV)** involves equipment that is an integral part of a weapon or weapons system; or

**(V)** subject to subparagraph (B), is critical to the direct fulfillment of military or intelligence missions; or

**(ii)** is protected at all times by procedures established for information that have been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.

**(B)** Subparagraph (A)(i)(V) does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications).

(3) The term "information technology" has the meaning given that term in section 11101 of title 40.

(Added Pub.L. 107-347, Title III, § 301(b)(1), Dec. 17, 2002, 116 Stat. 2947.)

➔§ 3543. Authority and functions of the Director

(a) **In general.**--The Director shall oversee agency information security policies and practices, including--

(1) developing and overseeing the implementation of policies, principles, standards, and guidelines on information security, including through ensuring timely agency adoption of and compliance with standards promulgated under section 11331 of title 40;

(2) requiring agencies, consistent with the standards promulgated under such section 11331 and the requirements of this subchapter, to identify and provide information security protections commensurate with the risk and magnitude of the harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of--

(A) information collected or maintained by or on behalf of an agency; or

(B) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency;

(3) coordinating the development of standards and guidelines under section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g-3) with agencies and offices operating or exercising control of national security systems (including the National Security Agency) to assure, to the maximum extent feasible, that such standards and guidelines are complementary with standards and guidelines developed for national security systems;

(4) overseeing agency compliance with the requirements of this subchapter, including through any authorized action under section 11303 of title 40, to enforce accountability for compliance with such requirements;

(5) reviewing at least annually, and approving or disapproving, agency information security programs required under section 3544(b);

(6) coordinating information security policies and procedures with related information resources management policies and procedures;

(7) overseeing the operation of the Federal information security incident center required under section 3546; and

(8) reporting to Congress no later than March 1 of each year on agency compliance with the requirements of this subchapter, including--

(A) a summary of the findings of evaluations required by section 3545;

(B) an assessment of the development, promulgation, and adoption of, and compliance with, standards developed under section 20 of the National Institute of Standards and Technology Act (15 U.S.C. 278g-3) and promulgated under section 11331 of title 40;

(C) significant deficiencies in agency information security practices;

(D) planned remedial action to address such deficiencies; and

(E) a summary of, and the views of the Director on, the report prepared by the National Institute of Standards and Technology under section 20(d)(10) of the National Institute of Standards and Technology Act (15 U.S.C. 278g-3).

**(b) National security systems.**--Except for the authorities described in paragraphs (4) and (8) of subsection (a), the authorities of the Director under this section shall not apply to national security systems.

**(c) Department of defense and central intelligence agency systems.**--(1) The authorities of the Director described in paragraphs (1) and (2) of subsection (a) shall be delegated to the Secretary of Defense in the case of systems described in paragraph (2) and to the Director of Central Intelligence in the case of systems described in paragraph (3).

(2) The systems described in this paragraph are systems that are operated by the Department of Defense, a contractor of the Department of Defense, or another entity on behalf of the Department of Defense that processes any information the unauthorized access, use, disclosure, disruption, modification, or destruction of which would have a debilitating impact on the mission of the Department of Defense.

(3) The systems described in this paragraph are systems that are operated by the Central Intelligence Agency, a contractor of the Central Intelligence Agency, or another entity on behalf of the Central Intelligence Agency that processes any information the unauthorized access, use, disclosure, disruption, modification, or destruction of which would have a debilitating impact on the mission of the Central Intelligence Agency.

(Added Pub.L. 107-347, Title III, § 301(b)(1), Dec. 17, 2002, 116 Stat. 2947.)

**⇒§ 3544. Federal agency responsibilities**

**(a) In general.**--The head of each agency shall--

**(1)** be responsible for--

**(A)** providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of--

**(i)** information collected or maintained by or on behalf of the agency; and

**(ii)** information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency;

**(B)** complying with the requirements of this subchapter and related policies, procedures, standards, and guidelines, including--

**(i)** information security standards promulgated under section 11331 of title 40; and

**(ii)** information security standards and guidelines for national security systems issued in accordance with law and as directed by the President; and

**(C)** ensuring that information security management processes are integrated with agency strategic and operational planning processes;

**(2)** ensure that senior agency officials provide information security for the information and information systems that support the operations and assets under their control, including through--

**(A)** assessing the risk and magnitude of the harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of such information or information systems;

**(B)** determining the levels of information security appropriate to protect such information and information systems in accordance with standards promulgated under section 11331 of title 40, for information security classifications and related requirements;

**(C)** implementing policies and procedures to cost-effectively reduce risks to an acceptable level; and



(D) periodically testing and evaluating information security controls and techniques to ensure that they are effectively implemented;

(3) delegate to the agency Chief Information Officer established under section 3506 (or comparable official in an agency not covered by such section) the authority to ensure compliance with the requirements imposed on the agency under this subchapter, including--

(A) designating a senior agency information security officer who shall--

(i) carry out the Chief Information Officer's responsibilities under this section;

(ii) possess professional qualifications, including training and experience, required to administer the functions described under this section;

(iii) have information security duties as that official's primary duty; and

(iv) head an office with the mission and resources to assist in ensuring agency compliance with this section;

(B) developing and maintaining an agencywide information security program as required by subsection (b);

(C) developing and maintaining information security policies, procedures, and control techniques to address all applicable requirements, including those issued under section 3543 of this title, and section 11331 of title 40;

(D) training and overseeing personnel with significant responsibilities for information security with respect to such responsibilities; and

(E) assisting senior agency officials concerning their responsibilities under paragraph (2);

(4) ensure that the agency has trained personnel sufficient to assist the agency in complying with the requirements of this subchapter and related policies, procedures, standards, and guidelines; and

(5) ensure that the agency Chief Information Officer, in coordination with other senior agency officials, reports annually to the agency head on the effectiveness of the agency information security program, including progress of remedial actions.

**(b) Agency program.**--Each agency shall develop, document, and implement an agencywide information security program, approved by the Director under section 3543(a)(5), to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source, that includes--

(1) periodic assessments of the risk and magnitude of the harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the agency;

(2) policies and procedures that--

(A) are based on the risk assessments required by paragraph (1);

(B) cost-effectively reduce information security risks to an acceptable level;

(C) ensure that information security is addressed throughout the life cycle of each agency information system; and

(D) ensure compliance with--

(i) the requirements of this subchapter;

(ii) policies and procedures as may be prescribed by the Director, and information security standards promulgated under section 11331 of title 40;

(iii) minimally acceptable system configuration requirements, as determined by the agency; and

(iv) any other applicable requirements, including standards and guidelines for national security systems issued in accordance with law and as directed by the President;

(3) subordinate plans for providing adequate information security for networks, facilities, and systems or groups of information systems, as appropriate;

(4) security awareness training to inform personnel, including contractors and other users of information systems that support the operations and assets of the agency, of--

(A) information security risks associated with their activities; and

(B) their responsibilities in complying with agency policies and procedures designed to reduce these risks;

(5) periodic testing and evaluation of the effectiveness of information security policies, procedures, and practices, to be performed with a frequency depending on risk, but no less than annually, of which such testing--

(A) shall include testing of management, operational, and technical controls of every information system identified in the inventory required under section 3505(c); and

(B) may include testing relied on in a evaluation [FN1] under section 3545;

(6) a process for planning, implementing, evaluating, and documenting remedial action to address any deficiencies in the information security policies, procedures, and practices of the agency;

(7) procedures for detecting, reporting, and responding to security incidents, consistent with standards and guidelines issued pursuant to section 3546(b), including--

(A) mitigating risks associated with such incidents before substantial damage is done;

(B) notifying and consulting with the Federal information security incident center referred to in section 3546; and

(C) notifying and consulting with, as appropriate--

(i) law enforcement agencies and relevant Offices of Inspector General;

(ii) an office designated by the President for any incident involving a national security system; and

(iii) any other agency or office, in accordance with law or as directed by the President; and

(8) plans and procedures to ensure continuity of operations for information systems that support the operations and assets of the agency.

**(c) Agency reporting.--**Each agency shall--

(1) report annually to the Director, the Committees on Government Reform and Science of the House of Representatives, the Committees on Governmental Affairs and Commerce, Science, and Transportation of the Senate, the appropriate authorization and appropriations committees of Congress, and the Comptroller General on the adequacy and effectiveness of information security policies, procedures, and practices, and compliance with the requirements of this subchapter, including compliance with each requirement of subsection (b);

(2) address the adequacy and effectiveness of information security policies, procedures, and practices in plans and reports relating to--

(A) annual agency budgets;

(B) information resources management under subchapter 1 [FN2] of this chapter;

(C) information technology management under subtitle III of title 40;

(D) program performance under sections 1105 and 1115 through 1119 of title 31, and sections 2801 and 2805 of title 39;

(E) financial management under chapter 9 of title 31, and the Chief Financial Officers Act of 1990 (31 U.S.C. 501 note; Public Law 101-576) (and the amendments made by that Act);

(F) financial management systems under the Federal Financial Management Improvement Act (31 U.S.C. 3512 note); and

(G) internal accounting and administrative controls under section 3512 of title 31, [FN3] (known as the "Federal Managers Financial Integrity Act"); and

(3) report any significant deficiency in a policy, procedure, or practice identified under paragraph (1) or (2)--

(A) as a material weakness in reporting under section 3512 of title 31; and

(B) if relating to financial management systems, as an instance of a lack of substantial compliance under the Federal Financial Management Improvement Act (31 U.S.C. 3512 note).

**(d) Performance plan.--**(1) In addition to the requirements of subsection (c), each agency, in consultation with the Director, shall include as part of the performance plan required under section 1115 of title 31 a description of--

(A) the time periods, and

(B) the resources, including budget, staffing, and training,

that are necessary to implement the program required under subsection (b).

(2) The description under paragraph (1) shall be based on the risk assessments required under subsection (b)(2)(1).

**(e) Public notice and comment.--**Each agency shall provide the public with timely notice and opportunities for comment on proposed information security policies and procedures to the extent that such policies and procedures affect communication with the public.

(Added Pub.L. 107-347, Title III, § 301(b)(1), Dec. 17, 2002, 116 Stat. 2949.)

[FN1] So in original. Probably should be "an".

[FN2] So in original. Probably should be "subchapter I".

[FN3] So in original. The comma probably should not appear.

**→§ 3545. Annual independent evaluation**

**(a) In general.--**(1) Each year each agency shall have performed an independent evaluation of the information security program and practices of that agency to determine the effectiveness of such program and practices.

**(2)** Each evaluation under this section shall include--

**(A)** testing of the effectiveness of information security policies, procedures, and practices of a representative subset of the agency's information systems;

**(B)** an assessment (made on the basis of the results of the testing) of compliance with--

**(i)** the requirements of this subchapter; and

**(ii)** related information security policies, procedures, standards, and guidelines; and

**(C)** separate presentations, as appropriate, regarding information security relating to national security systems.

**(b) Independent auditor.--**Subject to subsection (c)--

**(1)** for each agency with an Inspector General appointed under the Inspector General Act of 1978 or any other law, the annual evaluation required by this section shall be performed by the Inspector General or by an independent external auditor, as determined by the Inspector General of the agency; and

**(2)** for each agency to which paragraph (1) does not apply, the head of the agency shall engage an independent external auditor to perform the evaluation.

**(c) National security systems.--**For each agency operating or exercising control of a national security system, that portion of the evaluation required by this section directly relating to a national security system shall be performed--

**(1)** only by an entity designated by the agency head; and

(2) in such a manner as to ensure appropriate protection for information associated with any information security vulnerability in such system commensurate with the risk and in accordance with all applicable laws.

**(d) Existing evaluations.**--The evaluation required by this section may be based in whole or in part on an audit, evaluation, or report relating to programs or practices of the applicable agency.

**(e) Agency reporting.**--(1) Each year, not later than such date established by the Director, the head of each agency shall submit to the Director the results of the evaluation required under this section.

(2) To the extent an evaluation required under this section directly relates to a national security system, the evaluation results submitted to the Director shall contain only a summary and assessment of that portion of the evaluation directly relating to a national security system.

**(f) Protection of information.**--Agencies and evaluators shall take appropriate steps to ensure the protection of information which, if disclosed, may adversely affect information security. Such protections shall be commensurate with the risk and comply with all applicable laws and regulations.

**(g) OMB reports to Congress.**--(1) The Director shall summarize the results of the evaluations conducted under this section in the report to Congress required under section 3543(a)(8).

(2) The Director's report to Congress under this subsection shall summarize information regarding information security relating to national security systems in such a manner as to ensure appropriate protection for information associated with any information security vulnerability in such system commensurate with the risk and in accordance with all applicable laws.

(3) Evaluations and any other descriptions of information systems under the authority and control of the Director of Central Intelligence or of National Foreign Intelligence Programs systems under the authority and control of the Secretary of Defense shall be made available to Congress only through the appropriate oversight committees of Congress, in accordance with applicable laws.

**(h) Comptroller general.**--The Comptroller General shall periodically evaluate and report to Congress on--

- (1) the adequacy and effectiveness of agency information security policies and practices; and
- (2) implementation of the requirements of this subchapter.

(Added Pub.L. 107-347, Title III, § 301(b)(1), Dec. 17, 2002, 116 Stat. 2952, and amended Pub.L. 108-177, Title III, § 377(e), Dec. 13, 2003, 117 Stat. 2631.)

**➡§ 3546. Federal information security incident center**

**(a) In general.**--The Director shall ensure the operation of a central Federal information security incident center to--

(1) provide timely technical assistance to operators of agency information systems regarding security incidents, including guidance on detecting and handling information security incidents;

(2) compile and analyze information about incidents that threaten information security;

(3) inform operators of agency information systems about current and potential information security threats, and vulnerabilities; and

(4) consult with the National Institute of Standards and Technology, agencies or offices operating or exercising control of national security systems (including the National Security Agency), and such other agencies or offices in accordance with law and as directed by the President regarding information security incidents and related matters.

**(b) National security systems.**--Each agency operating or exercising control of a national security system shall share information about information security incidents, threats, and vulnerabilities with the Federal information security incident center to the extent consistent with standards and guidelines for national security systems, issued in accordance with law and as directed by the President.

(Added Pub.L. 107-347, Title III, § 301(b)(1), Dec. 17, 2002, 116 Stat. 2954.)

**➡§ 3547. National security systems**

The head of each agency operating or exercising control of a national security system shall be responsible for ensuring that the agency--

(1) provides information security protections commensurate with the risk and magnitude of the harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information contained in such system;

(2) implements information security policies and practices as required by standards and guidelines for national security systems, issued in accordance with law and as directed by the President; and

(3) complies with the requirements of this subchapter.

(Added Pub.L. 107-347, Title III, § 301(b)(1), Dec. 17, 2002, 116 Stat. 2954.)

#### **⇒§ 3548. Authorization of appropriations**

There are authorized to be appropriated to carry out the provisions of this subchapter such sums as may be necessary for each of fiscal years 2003 through 2007.

(Added Pub.L. 107-347, Title III, § 301(b)(1), Dec. 17, 2002, 116 Stat. 2954.)

#### **⇒§ 3549. Effect on existing law**

Nothing in this subchapter, section 11331 of title 40, or section 20 of the National Standards and Technology Act (15 U.S.C. 278g-3) may be construed as affecting the authority of the President, the Office of Management and Budget or the Director thereof, the National Institute of Standards and Technology, or the head of any agency, with respect to the authorized use or disclosure of information, including with regard to the protection of personal privacy under section 552a of title 5, the disclosure of information under section 552 of title 5, the management and disposition of records under chapters 29, 31, or 33 of title 44, the management of information resources under subchapter I of chapter 35 of this title, or the disclosure of information to the Congress or the Comptroller General of the United States. While this subchapter is in effect, subchapter II of this chapter shall not apply.

(Added Pub.L. 107-347, Title III, § 301(b)(1), Dec. 17, 2002, 116 Stat. 2955.)